Fraud, Waste & Abuse
A Message from the Compliance Office…

The federal government has shown a strong commitment to eliminating fraud, waste and abuse (FWA) within federal programs, and to holding individuals and entities accountable for violations of the law. This includes healthcare.

The OIG Strategic Plan 2025-2030 establishes three clear goals. Note the #1 goal:

1. **Fight fraud, waste, and abuse**
2. Promote quality, safety and value
3. Advance excellence and innovation.

These goals will guide OIG to "carry out its mission to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of HHS programs as well as the health and welfare of the people they serve."

In addition, it has been reported that CMS will begin auditing all eligible Medicare Advantage contracts. They will be expediting their efforts to increase auditing numbers through an expanded workforce and enhanced technology.

While the report addresses RADV audits, there is a trickle-down effect that will now pose the potential audit for all of us, regardless of status.

All of this illustrates how **extremely important** it is for UBMD personnel to be able to recognize improper conduct, and how to prevent it and correct it.

UB|MD
PHYSICIANS' GROUP

Training Requirements

In order to meet Fraud, Waste & Abuse (FWA) training requirements set by The Centers for Medicare and Medicaid Services (CMS), **all** UBMD providers and staff are **required** to complete FWA training within 30 days of hire, **and** annually thereafter.

This training program is developed from the CMS web-training program to ensure all required information is included.

UB|MD
PHYSICIANS' GROUP

Training Objectives

Once training is complete, you should be able to:

- ✓ Recognize & distinguish Fraud, Waste & Abuse;
- ✓ Recognize major laws & regulations pertaining to FWA;
- ✓ Understand potential consequences & penalties for violations;
- ✓ Identify & apply methods of preventing FWA;
- ✓ Know how to report FWA; and
- ✓ Determine how best to correct FWA.

UB|MD
PHYSICIANS' GROUP

Why do we need FWA training?

- Learn how to detect, correct and prevent FWA.
  - ✓ Prevent improper conduct, whether intentional or not, from occurring.
  - ✓ Detect and prevent patterns of improper conduct, or the appearance of improper conduct, from occurring.
- Billions of dollars are spent improperly every year due to fraud, waste & abuse.
- As healthcare workers and UBMD employees, whether provider or administrative, we are ALL responsible for combatting fraud, waste & abuse.
- Any of our actions determined to be fraud, waste or abuse can lead to financial losses not only to government programs, but to your practice plans and you as well, including fines, penalties, exclusion and imprisonment,
- **To be part of the solution!**

UB|MD
PHYSICIANS' GROUP

What is Fraud?

- **Fraud**
  - ✓ Requires willingness, intent, knowledge.
  - ✓ Knowingly submitting false claims, or causing false claims to be submitted;
  - ✓ Knowingly making misrepresentations of fact to get a federal health care payment when no other entitlement would exist;
  - ✓ Knowingly soliciting, getting, offering, or making payments (kickbacks, bribes, rebates) to encourage or reward referrals for items or services reimbursed by federal health care programs;
  - ✓ Knowingly and willfully executing, or attempting to execute, a scheme or lie to defraud ANY health care benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) money or property owned by, or controlled by, any health care benefit program.

UB|MD
PHYSICIANS' GROUP

What is Fraud (continued)?

- **Examples**
  - ✓ Knowingly billing for services of higher complexity than services actually provided or documented.
  - ✓ Knowingly billing for services or supplies not provided.
  - ✓ Knowingly ordering medically unnecessary patient items or services.
  - ✓ Offering money or favors for patient referrals or to influence purchasing.
  - ✓ Billing Medicare for appointments patients don't keep.
  - ✓ Knowingly altering claims forms, medical records, or receipts to receive a higher payment.

UB|MD
PHYSICIANS' GROUP

What is Abuse?

- **Abuse**
  - ✓ Practices that directly or indirectly result in unnecessary costs to the Medicare Program.
  - ✓ Any practice that doesn't provide medically necessary services or doesn't meet professionally recognized standards of care.

- **Examples**
  - ✓ Billing unnecessary medical services.
  - ✓ Charging excessively for services or supplies.
  - ✓ Misusing codes on a claim, like upcoding or unbundling codes.
  - ✓ Not following HIPAA guidelines for protecting a patient's PHI.

UB|MD
PHYSICIANS' GROUP

What is Waste?

- **Waste**
  - ✓ Practices that directly or indirectly results in unnecessary costs to the Medicare Program, such as overusing services.
  - ✓ Generally not caused by criminally negligent actions, but by misuse of resources.

- **Examples**
  - ✓ Conducting excessive office visits or writing excessive prescriptions.
  - ✓ Prescribing more medications than necessary to treat a specific condition.
  - ✓ Ordering excessive lab tests.

UB|MD
PHYSICIANS' GROUP

Difference Between Fraud, Waste & Abuse

Intent, knowledge, and willingness are the primary differences.

- Fraud requires intent to obtain payment, and knowledge that the actions are wrong.
- Waste & Abuse may involve obtaining improper payment or creating unnecessary cost to Medicare Program, but do not require the same intent and knowledge.

For the definitions of fraud, waste & abuse, refer to Chapter 21 Section 20 of the "Medicare Managed Care Manual" and Chapter 9 of the "Prescription Drug Benefit Manual" on the Centers for Medicare & Medicaid Services (CMS) website

UB|MD
PHYSICIANS' GROUP

Laws & Penalties

To detect FWA, you need to know the key laws involved:

- Federal False Claims Act (FCA)
- Anti-Kickback Statute (AKS)
- Physician Self-Referral Law (Stark Statute)
- Fraud Statute
- Exclusion Statute
- Civil Monetary Penalties Law (CMPL)
- Health Insurance Portability and Accountability Act (HIPAA)

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
False Claims Act (FCA)

- False Claims Act: Makes a person liable to pay damages to the government if they knowingly:
  - ✓ Conspire to violate the FCA;
  - ✓ Carry out other acts to get government property my misrepresentation;
  - ✓ Conceal or improperly avoid or decrease an obligation to pay the government;
  - ✓ Make or use a false record or statement supporting a false claim;
  - ✓ Present a false claim for payment or approval.
- Actual Example:
  - ✓ A physician practice hired an outside company to review medical records to find additional diagnosis codes it could submit to increase CMS risk capitation payments.
  - ✓ The company informed the practice that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported.
  - ✓ Practice failed to report the unsupported diagnosis codes to Medicare.
  - ✓ Practice agreed to pay $22.6 million to settle FCA allegations.
- Penalties May Include:
  - ✓ Fines, imprisonment, or both
  - ✓ Recovery up to 3 times amount of government's damages due to the false claims plus $11,000 per false claim filed.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Anti-Kickback Statute (AKS)

- The Anti-Kickback Statute: Makes it a crime to knowingly and willfully offer, pay, solicit or receive any remuneration directly or indirectly to encourage or reward patient referrals or business generation involving any item or service payable by a federal health care program.
  - ✓ Remuneration includes anything of value, such as cash, free rent, expensive hotel stays and meals, and excessive compensation for medical directorships or consultations.
  - ✓ Safe harbors may apply.

- Actual Example:
  - ✓ A physician operating a pain management practice conspired to solicit and get kickbacks for prescribing a highly addictive version of the opioid fentanyl, and reported that patients had breakthrough cancer pain to secure insurance payments.
  - ✓ Received $180,000 in speaker fee kickbacks from the drug manufacturer.
  - ✓ Admitted the scheme cost Medicare and other payers more than $750,000.
  - ✓ Was required to pay restitution.

- Penalties may include:
  - ✓ Fine and/or imprisonment up to 10 years

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Physician Self-Referral Law (Stark Law)

- The Physician Self-Referral Law (Stark Law): Prohibits a physician from referring certain designated health services (DHS) to an entity where the physician, or an immediate family member, has an ownership/investment interest or has a compensation arrangement, unless an exception applies.
- Designated Health Services include:
  - ✓ Clinical lab services
  - ✓ Physical therapy, occupational therapy, and outpatient speech-language pathology services
  - ✓ Radiology and other imaging services
  - ✓ DME and supplies
  - ✓ Parenteral and enteral nutrients, equipment, and supplies
  - ✓ Prosthetics, orthotics, and supplies
  - ✓ Home health services
  - ✓ Outpatient prescription drugs
  - ✓ Inpatient and outpatient hospital services.
- Penalties may include:
  - ✓ Fines, repayment of claims, and potential exclusion from participation in Federal health care programs.
- Actual Example:
  - ✓ A hospital was ordered to pay more than $3.2 million to settle Stark Law violations for maintaining 97 financial relationships with physicians and physician groups outside the fair market value standards or that were improperly documented exceptions.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
The Fraud Statute

- The Fraud Statute prohibits knowingly and willfully executing, or attempting to execute, a scheme about the delivery of, or payment for, health care benefits, items or services to:
  - ✓ Defraud any health care benefit program; or
  - ✓ Obtain by means of false or fraudulent pretenses, representations or promises, any money or property owned by or under control of any health care benefit plan.
  - ✓ Conviction does not require proof that the violator had knowledge of the law or specific intent to violate the law.

- Penalties may include:
  - ✓ Fines, prison, or both.

- Actual Example:
  - ✓ A pharmacist submitted claims for nonexistent prescriptions and drugs not dispensed, pleaded guilty to health care fraud, and got a 15-month prison sentence and was ordered to pay more than $166,000 in restitution to the plan.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Exclusion Statute

- Exclusion Statute: Requires OIG to exclude health care providers and suppliers convicted of these criminal offenses from participating in all federal health care programs:
  - ✓ Medicare or Medicaid fraud, including offenses related to delivering Medicare or Medicaid items or services;
  - ✓ Patient abuse or neglect;
  - ✓ Felony convictions for other health care-related fraud or theft, or other financial misconduct; and
  - ✓ Felony convictions relating to unlawful manufacture, distribution, prescription or dispensing of controlled substances.
- The OIG also maintains the List of Excluded Individuals and Entities (LEIE website.
- The U.S. General Services Administration (GSA) administers the Excluded Parties List (EPLS), which enables various federal agencies, including the OIG, to take debarment actions.
- Both the LEIE and EPLS should be checked when looking for excluded individuals and entities as the lists are not the same.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Exclusion Statute

- Exclusion Statute (Continued)
  - ✓ Excluded providers may not participate in the Federal health care programs for a designated period. If excluded by the OIG, then Federal health care programs, including Medicare and Medicaid, will not pay for items or services that you furnish, order or prescribe.
  - ✓ Excluded providers may not bill directly for treating Medicare and Medicaid patients, and an employer of a group practice may not bill for an excluded provider's services.
  - ✓ At the end of an exclusion period, an excluded provider must seek reinstatement as reinstatement is not automatic.
  - ✓ Mandatory exclusions stay in effect for a minimum of 5 years, but can be longer, or even permanent.

- Permissive Exclusion: OIG may impose exclusions for offenses not under a mandatory exclusion. Permissive exclusions vary in length. Examples include, but are not limited to:
  - ✓ Misdemeanor health care fraud convictions other than Medicare or Medicaid fraud;
  - ✓ Misdemeanor convictions for unlawfully manufacturing, distributing, prescribing or dispensing controlled substances;

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Exclusion Statute

- Permissive Exclusion (Continued)

  - ✓ Revocation, suspension or health care license surrender for reasons of professional competence, professional performance, or financial integrity;
  - ✓ Providing unnecessary or substandard service;
  - ✓ Convictions for obstruction an investigation or audit;
  - ✓ Engaging in unlawful kickback arrangements;
  - ✓ Defaulting on health education loan or scholarship obligations.

***

- The UBMD Compliance Plan requires that all practices who bill government programs including, without limitation, Medicare and Medicaid, to check the names of all providers, staff and agents/vendors against exclusionary databases regularly.

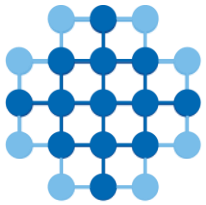
  - ✓ Check Monthly:
    - OIG-LEIE, GSA-SAM, and OMIG-List
  - ✓ Check when a provider is credentialed or re-credentialed:
    - SDN List, NPPES, and Death Master

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Civil Monetary Penalties Law (CMP)

- Civil Monetary Penalties Law (CMP) authorizes the OIG to seek civil monetary penalties, and sometimes exclusions, for a variety of health care fraud violations, including:

  - ✓ Arranging for an excluded individual's or entity's services or items;
  - ✓ Failing to grant OIG timely access to records;
  - ✓ Filing a claim you know or should know is for an item or service that wasn't provided as claimed, or is false or fraudulent;
  - ✓ Filing a claim you know or should know is for an unpayable item or service;
  - ✓ Violating the AKS;
  - ✓ Violating the Medicare physician agreement;
  - ✓ Providing false or misleading information expected to influence a discharge decision;
  - ✓ Failing to provide an adequate medical screening exam for patients who present to a hospital ED with an emergency medical condition or in labor;
  - ✓ Making false statements or misrepresentations on applications or contracts to participate in federal health care programs.



UB|MD
PHYSICIANS' GROUP

Laws & Penalties
Civil Monetary Penalties Law (CMP)

- Damages & Penalties:
  - ✓ Vary based on the type & severity of violation.
  - ✓ Approximately $10,000-$100,000 per violation.
  - ✓ Also subject to up to 3 times the amount claimed for each service or item, or up to 3 times the amount of remuneration offered, paid, solicited or received.

- Actual example:
  - ✓ A pharmacy and its owner agreed to pay over $1.3 million to settle allegations they submitted unsubstantiated Part D claims for brand name prescription drugs the pharmacy couldn't have dispensed based on inventory records.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties
HIPAA

- Health Insurance Portability & Accountability Act (HIPAA):
  - ✓ Created greater access to health care insurance.
  - ✓ Strengthened protection of privacy of health care data.
  - ✓ Promoted standardization and efficiency in the health care industry.
  - ✓ Deters unauthorized access to protected health information (PHI).
  - ✓ Anyone with access to PHI, must comply with HIPAA.
- Damages & Penalties:
  - ✓ Violations may result in Civil Monetary Penalties.
  - ✓ In some cases, criminal penalties may apply.
- Actual Example:
  - ✓ A former hospital employee pleaded guilty to criminal HIPAA charges after getting PHI with the intent to use it for personal gain. He was sentenced to 12 months and 1 day in prison.

UB|MD
PHYSICIANS' GROUP

Laws & Penalties

In summary, beyond paying restitution to CMS for fraudulently obtained payments, fraud and abuse penalties can include exclusions, civil monetary penalties, and sometimes criminal sanctions, which include fines and prison, against health care providers and suppliers who violate the False Claims Act, Anti-Kickback Statute, Stark Law, or Fraud Statute.

UB|MD
PHYSICIANS' GROUP

What are your responsibilities?

- You play a vital role in preventing, detecting and reporting potential FWA, as well as Medicare non-compliance.
- You must comply with all applicable statutory, regulatory and other Medicare requirements, including adopting and using an effective compliance program.
- You have a duty to report any compliance concerns as well as any suspected or actual violations of which you may be aware.
- You have a duty to follow the UBMD Compliance Plan, including the Code of Conduct, which articulates UBMD's commitment to standards of conduct and ethical rules of behavior.

UB|MD
PHYSICIANS' GROUP

What is a Whistleblower?

- A whistleblower is a person who exposes information or activity deemed illegal, dishonest or violate professional or clinical standards.
- Whistleblowers are protected from retaliation.
- Whistleblowers may receive at least 15% but not more than 30% of money collected in successful lawsuit.

UB|MD
PHYSICIANS' GROUP

How can you prevent FWA?

- Conduct yourself in an ethical manner at all times.
- Provide only medically necessary services.
- Use accurate and complete documentation that supports claims.
- Ensure accurate and timely coding and billing.
- Comply with other payers' rules.
- Verify all information provided to you.
- Be aware of suspicious activity.
- Keep up to date with FWA & UBMD policies and procedures, standards of conduct, laws, regulations, CMS guidance and UBMD Compliance Office guidance.
  - ✓ Read and understand the UBMD Compliance Plan.
  - ✓ Read newsletters and other communications sent to you from the UBMD Compliance Office as they contain important information and updates.
  - ✓ Complete all compliance training as required.
  - ✓ Know that reported issues will be addressed.

UB|MD
PHYSICIANS' GROUP

Reporting FWA

- Everyone is *required* to report *known or suspected* instances of FWA.
  - ✓ Retaliation for reporting compliance concerns in good faith will not be tolerated, regardless of whether or not a violation is found as a result of the initial report.
  - ✓ This, and the process for reporting, is clearly stated in the UBMD Compliance Plan.
- Any concerns should be reported to your supervisor and/or the UBMD Compliance Office.
  - ✓ Even if you suspect something is wrong but aren't sure if it is FWA, report it.
  - ✓ Contact the Compliance Office directly.
  - ✓ Utilize the Compliance Hotline (716.888.4752) or Compliance Issue Reporting Form.
    - o You may remain anonymous if you wish.
  - ✓ All reported concerns will be investigated by the Chief Compliance Officer.

UB|MD
PHYSICIANS' GROUP

Reporting FWA

- When reporting suspected FWA, you should include:
  - ✓ Contact information for the source of information, suspects & witnesses;
  - ✓ Details of the alleged FWA;
  - ✓ Identification of specific rules allegedly violated; and
  - ✓ The suspect's history of compliance, education training and communication within UBMD and other entities.

- If warranted, potentially fraudulent conduct must be reported to government authorities such as OIG, DOJ or CMS.
  - ✓ **The UBMD Chief Compliance Officer should ALWAYS be contacted first regarding cases of self-disclosure.**
  - ✓ Individuals or entities who wish to voluntarily disclose self-discovered potential fraud to OIG may do so under Self-Disclosure Protocol (SDP), which the UBMD Chief Compliance Officer will guide you through.
  - ✓ Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a government directed investigation and civil or administrative litigation.

UB|MD
PHYSICIANS' GROUP

Correcting FWA

- Once FWA is detected, it must promptly be corrected.
- Correcting the problem saves the government (and very possibly your practice) money, and ensures that you are in compliance with CMS requirements.
- Always consult the UBMD Chief Compliance Officer to find out the process for corrective action plan development, and develop a plan.
- Actual corrective plan will vary, depending on the specific circumstances, but in general:
  - ✓ Design the corrective action to correct the underlying problem that results in FWA program violations and prevents future non-compliance.
  - ✓ Tailor the corrective action to address the particular FWA, problem, or deficiency identified.
  - ✓ Include timeframe for specific actions.
  - ✓ Document corrective actions addressing non-compliance or FWA committed by the employee, and include consequences for failure to satisfactorily complete the corrective action.
  - ✓ Once started, continually monitor corrective actions to ensure they are effective.

UB|MD
PHYSICIANS' GROUP

Correcting FWA

- Corrective action will depend on the specific circumstances, but may include:
  - ✓ Adopting new prepayment edits or document review requirements;
  - ✓ Conducting additional mandated training;
  - ✓ Providing educational materials;
  - ✓ Revising policies and/or procedures;
  - ✓ Sending warning letters;
  - ✓ Terminating an employee or provider;
  - ✓ Any combination of the above.

UB|MD
PHYSICIANS' GROUP

Compliance Hotline

UBMD COMPLIANCE HOTLINE

716-888-4752

COMPLETELY ANONYMOUS

. Report known, suspected or potential fraud, abuse, problems, concerns.

. Report HIPAA-related concerns.

. Report other compliance issues or concerns.

. Ask questions; request guidance (you will need to provide contact info to receive answers).

. Provide relevant information: Date(s), time(s), department, behavior in question, person(s) in question.

. You are welcome to provide contact information if you wish, but you may remain anonymous if preferred.

UBMD Compliance Office
665 Main St., 2nd Floor
Buffalo, NY 14203

Larry DiGiulio,
Chief Compliance Officer

Sue Marasi,
Compliance Administrator

- UBMD's non-retaliation policy will be strictly adhered to.

. This is a voice mail box that is monitored during regular business hours, but is accessible for reporting 24 hours, 7days a week.

. If there is an IMMEDIATE THREAT to person or property is involved, please DO NOT LEAVE MESSAGE on this line.
Contact your direct supervisor immediately!

UB|MD
PHYSICIANS' GROUP

For more information…

- False Claims Act: 31 United States Code (U.S.C.) Sections 3729-3733
- Fraud Statute: 18 USC Sections 1346-1347
- Anti-Kickback Statute: 42 USC Section 1320a-7b(b)
- Safe Harbors: 42 CFR Section 1001.952
- Stark Statute (Physician Self-Referral Law): 42 USC Section 1395nn
- Civil Monetary Penalties: 42 USC 1320a-7a and the Act, Section 1128A(a)
- Exclusion: LEIE and EPLS and 42 USC Section 1320a-7 and 42 Code of Federal Regulations (CFR) Section 1001.1901
- HIPAA: HIPAA Webpage

UB|MD
PHYSICIANS' GROUP

Questions

REMEMBER!!!

Compliance & fraud prevention are **everyone's responsibility** - governing board, management, providers, and staff.

If you have any questions regarding this training, please contact:

Larry DiGiulio, Chief Compliance Officer
larryd@buffalo.edu

or

Sue Marasi, CHC, CPCA
Compliance Administrator
smmarasi@buffalo.edu

ANONYMOUS COMPLIANCE HOTLINE

716-888-4752

UB|MD
PHYSICIANS' GROUP

HIPAA Training

UB|MD
PHYSICIANS' GROUP

HIPAA Training Agenda

- What is HIPAA?
- HIPAA Enforcement
- Protected Health Information (PHI)
- Privacy Rule
- Patients' Rights
- Minimum Necessary
- Notice of Privacy Practice (NPP)
- Pediatric Patients
- Security Rule
- Three HIPAA Security Safeguards
- Breach Notification Rule
- Information Blocking
- Business Associates Agreement
- Cell Phone & Email Usage
- Important HIPAA Reminders
- Reporting HIPAA Violations
- HIPAA Case Examples

UB|MD
PHYSICIANS' GROUP

What is HIPAA?

HIPAA stands for:

- Health
- Insurance
- Portability and
- Accountability
- Act

HIPAA is a broad Federal Law that establishes basic privacy protections to which all patients in the United States are entitled. It gives them the right to access their own health records, and to have their health information kept private and secure.

HIPAA establishes standards to safeguard the protected health information (PHI) that you hold if you are one of these covered entities or their business associate:

- Health plan
- Health care clearinghouse
- Health care provider/hospital/organization

UB|MD
PHYSICIANS' GROUP

HIPAA Enforcement

The Office of Civil Rights (OCR) enforces HIPAA Rules.

OCR will watch and enforce the following:

- Unpermitted PHI use and disclosures.
- Use and disclosure of more than the **minimum necessary** PHI.
- Lack of PHI safeguards.
- Lack of Administrative, Technical, and Physical ePHI Safeguards.
- Lack of patients' access to their PHI.

❖ This is **not an exclusive list** to OCR enforcement actions.

UB|MD
PHYSICIANS' GROUP

Protected Health Information (PHI)

Information is considered protected health information if you hold or transmit it in any form, including electronic, paper, or verbal.

PHI includes information regarding:

- Eighteen Common Identifiers
  - Can you recreate the patient information with 4 or fewer identifiers?
- The patient's past, present, and future physical or mental health condition.
- Medical records
  - Diagnosis codes, test results, doctor notes
- Documentation
  - Appointment scheduling notes
  - Prescription records
  - Health-related emails
- Billing/Payment information
  - Claims
  - Payment history
  - Health plan beneficiary numbers

UB|MD
PHYSICIANS' GROUP

PHI: 18 Common Identifiers

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

UB|MD
PHYSICIANS' GROUP

Primary Rules of HIPAA

HIPAA is built on three primary rules:

- **Privacy Rule**
  Sets the standard for who can look at and receive patients' PHI.
- **Security Rule**
  Outlines the safeguards that must be put in place by healthcare organizations to keep patients' digital data safe from hackers and unauthorized access.
- **Breach Notification Rule**
  Mandates accountability if PHI is compromised in a data breach.

UB|MD
PHYSICIANS' GROUP

The Privacy Rule

The Privacy Rule protects patients' protected health information (PHI) and allows you to exchange information and coordinate your patient's care securely, and shifts control of health data back to the individual.

The Privacy Rule:

- Covers all forms of PHI, whether spoken, written on paper, or transmitted electronically.
- Dictates that healthcare providers and insurance companies can generally only share patient information for treatment, payment, and healthcare operations unless the patient gives them explicit written permission.

UB|MD
PHYSICIANS' GROUP

Patients' Rights

Patients have several different rights under the privacy rule, some of which are the following:

- Examine and receive a copy of their medical record, including an electronic copy of their medical records within 10 days in New York State.
- Request corrections to their medical records, and receive a response to the request. Provider must respond to such a request within 60 calendar days.
- Limit their plan's access to information about treatments they paid cash for.

NOTE: Under the Privacy Rule, you are allowed to report child abuse or neglect to the authorities.

UB|MD
PHYSICIANS' GROUP

Minimum Necessary

In HIPAA Privacy, the Minimum Necessary Rule is often referred to as the Golden Rule. This means sharing only the essential amount of PHI required to perform a specific task.

HIPAA requires healthcare workers to use or share only the minimum necessary information to perform their job duties.

Ask yourself these important questions when looking at private health information:

1. Do I need this information to perform my job and provide good patient care?
2. What is the least amount of information I need to perform my job?

If you find you do not have the access that you have, then let your supervisor immediately know.

UB|MD
PHYSICIANS' GROUP

Minimum Necessary

"Minimum Necessary" Keys:

- **Limit Access:** Only employees who ***need*** the information to do their jobs should have access to it.
- **Limit Disclosure:** Share only the ***minimum amount*** of PHI required to achieve a specific purpose.
- **Exceptions:** This rule does ***not*** apply when sharing information with other providers for a patient's treatment or when a patient requests their own records.

UB|MD
PHYSICIANS' GROUP

Notice of Privacy Practices

The Privacy Rule Requires that we notify patients about their privacy rights and how you use and share their information. This is called a Notice of Privacy Practices, and the patient must receive this at the time of their first appointment or prior to that appointment.

- The patient does not have to sign the Notice of Privacy Practices, also known as the "acknowledgment of receipt of the notice."
- The provider must keep the NPP on file, either with the signed attestation or notation of the patient's refusal to sign.
- Not signing the NPP does not give the provider rights to disclose privacy information. The patient is still protected under HIPAA.

UB|MD
PHYSICIANS' GROUP

Pediatric Patients

Navigating the intersection of federal HIPAA regulations and New York State (NYS) laws for pediatric patients involves balancing parental rights with the growing privacy rights of the minor. In New York, the rules often lean toward protecting the minor's confidentiality as they approach adolescence.

Questions often arise regarding:

- Authorized signatories and personal representatives
- Identifications & documentation requirements
- Records release
- Custody and guardianship considerations

UB|MD
PHYSICIANS' GROUP

Pediatric Patients:
Authorized Signatories & Personal Representatives

For most minors, the parent or legal guardian is the default representative and can sign for the release of records.

New York State Specifics:

- Joint Custody: Either parent can typically sign for records unless a court order explicitly says otherwise.
- Sole Custody: The custodial parent has decision-making authority, but the non-custodial parent still has a right to access records unless parental rights have been terminated, or a court order specifically prohibits access.
- Foster Parents: Generally **cannot** sign for the release of records. This authority usually remains with the local Department of Social Services (DSS) commissioner or the biological parent (if rights are intact).
- Temporary Caregivers: NYS allows a "Designation of Person in Parental Relationship" form, which permits a non-parent (like a grandparent) to consent to treatment and access records for up to six months.

Before giving PHI to anyone, always check for and carefully review waivers and/or court orders on file.

UB|MD
PHYSICIANS' GROUP

Pediatric Patients: Identification & Documentation Requirements

To obtain minors' records in NYS, providers **require** proper identification.

- **Requestor's Photo ID:** Valid state-issued driver's license, non-driver ID, or passport. Always be sure to check ID!
- **Proof of Relationship:**
  - **Minor's Birth Certificate:** Frequently required to prove the parent-child link if the parent is not already on file.
  - **Court Orders:** Documentation of legal guardianship, adoption papers, or specific custody agreements if there are restrictions on either parent.
- **Written Request:** Must have a completed and signed "Authorization for Release of Health Information Pursuant to HIPAA" (OCA Official Form No.: 960) to disclose PHI to third parties such as family members, attorneys, or insurers.

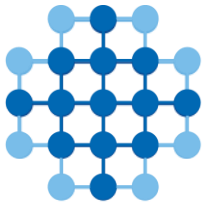
Before giving PHI to anyone, always check for and carefully review waivers and/or court orders on file.

UB|MD
PHYSICIANS' GROUP

Pediatric Patients: "12-Year-Old Rule" in New York

NYS Public Health Law contains a unique provision regarding minors and their records:

- **Notification:** If a parent/guardian requests the records of a minor **over the age of 12**, the provider **may notify** the minor of the request.
- **Right to Object:** If the minor objects to the disclosure, the provider has the discretion to **deny the parent's request** for access, provided the provider believes disclosure would be detrimental to the provider-patient relationship or the minor's care.



UB|MD
PHYSICIANS' GROUP

Pediatric Patients:
Minor-Consented Services

In New York State, when a minor is legally allowed to consent to their own care in NYS, **they control the record**. Parents do not have an automatic right to see records related to:

- **Reproductive Health:** Pregnancy tests, prenatal care, and abortion.
- **Sexual Health:** STI/HIV testing and treatment (minors of any age can consent to STI care).
- **Substance Abuse:** Treatment for alcohol or drug dependency.
- **Mental Health:** Outpatient services (if the provider determines the minor is "mature enough" and involving parents would be detrimental).

Also in New York State, many patient portals cut off or limit parental access once the child hits 12 or 23 years of age to protect teen privacy.

Note on Waivers: For a parent to see these "sensitive" records, the minor must sign a specific waiver or authorization and specifically initial the sections for HIV, mental health, or substance abuse.

UB|MD
PHYSICIANS' GROUP

Security Rule

While the Privacy Rule covers *who* is allowed to see medical data, the Security Rule focuses on the *how* – the security measures needed to defend digital health data against breaches, accidents, and hackers.

The Security Rule is anchored by the security concept known as the CIA Triad - Confidentiality, Integrity, and Availability. In healthcare, it is sometimes referred to as the HIPAA Triad, and translates as follows:

- Confidentiality: Restricting access to ePHI so only authorized people can see it.
  - *Example*: Using multi-factor authentication and data encryption so a lost laptop doesn't lead to exposed patient records.
- Integrity: Ensuring that patient data is accurate and has not been improperly altered.
  - *Example*: Keeping tracking systems (auditing) to see exactly who edited, or even viewed, a patient's chart and when.
- Availability: Making sure authorized users can get to the data when they need it.
  - *Example:* Having ironclad data backups and disaster recovery plans in place to providers can still treat patients during power outages or a ransomware attack.

UB|MD
PHYSICIANS' GROUP

Security Rule

The Security Rule includes security requirements to:

- Develop reasonable and appropriate security policies for your organization.
- Ensure Confidentiality, Integrity, and Availability of all ePHI you create, get, maintain, or transmit.
- Identify and protect against threats to ePHI security or integrity.
- Protect against impermissible uses or disclosures
- Analyze security risks in your environment and create appropriate solutions.
- Review and modify security measures to continue protecting ePHI in a changing environment.
- ENSURE EMPLOYEE COMPLIANCE.

UB|MD
PHYSICIANS' GROUP

Three HIPAA Security Safeguards

HIPAA security has many layers of protection, and within these layers of protection are certain safeguards that covered entities must comply with to reasonable standards. They are the following:

- **Administrative Safeguard**: This includes workforce training, risk analysis, management, HIPAA Information Security Officer, Incident Response Management, and Disaster Response Planning.
- **Physical Safeguard:** These are defined as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." This would include:
  - Facility access controls
  - Workstation security (making sure computer monitors containing patient charts aren't visible to the waiting room, or others who shouldn't have access to them)
  - Mobile device security.
- **Technical Safeguard**: These are technology-based methods used to protect ePHI and control access to it. For example, Access controls, Audit Controls, Firewall Security, Data back up, and device and media Controls.

UB|MD
PHYSICIANS' GROUP

Breach Notification Rule

If you think you might have a breach, **IMMEDIATELY** call the Compliance Office and ask for assistance.

If a PHI breach is experienced, you must follow the Breach Notification Rule. The rule requires you to notify affected patients, HHS, and, in some cases, the media, depending on the number of affected individuals.

What is a breach?

Generally, a breach is an unpermitted use and disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach UNLESS there is a LOW probability the PHI has been compromised, based on a risk assessment of the following:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or got the disclosed PHI.
- Whether an individual acquired or viewed the PHI.
- The extent to which you reduced the PHI risk.

UB|MD
PHYSICIANS' GROUP

Breach Notification Rule

HHS (Health and Human Services) Notification of Breach Information:

1. A Provider or Organization must notify authorities of most breaches without reasonable delay and no later than 60 days after discovering the breach.
2. Submitting notifications of smaller breaches affecting fewer than 500 patients to HHS can be done annually.
3. Greater than 500 patients by Covered Entities (CE) are required to provide notice to prominent media outlets serving the state jurisdiction. This will be in the form of a press release to appropriate media outlets serving the affected area. It must also be done in a timely manner and within 60 days.
4. The Breach Notification also requires Business Associates to notify you of breaches at or by the Business Associate.

Further information can be found on the HHS site under the following link:

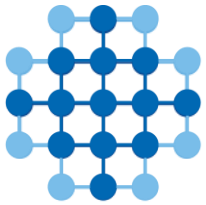
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

UB|MD
PHYSICIANS' GROUP

Information Blocking

Most clinical information is digitized, accessible, and shareable thanks to several technology and policy advances making interoperable, electronic health record systems widely available. In 2016, the 21st Century Cures Act (Cures Act) made sharing electronic health information the expected norm in health care by authorizing the Secretary of Health and Human Services (HHS) to identify "reasonable and necessary activities that do not constitute information blocking." The Office of National Coordinator for Health Information Technology (ONC) 2020 Cures Act Final Rule established information-blocking exceptions to implement the law.

Interfering with or blocking access, exchange, or use of electronic health information (EHI) except as required by law will prompt an investigation by HHS.



UB|MD
PHYSICIANS' GROUP

Business Associate Agreement

What is a HIPAA Business Associate Agreement (BAA)?

- Most often a BAA is a contract between a HIPAA-covered entity (CE) and a business or individual that performs certain function(s) or activities on behalf of, or provides a service to, the covered entity when the function, activity, or service involves the creation, receipt, maintenance or transmission of Protected Health Information (PHI).
- A Business Associate must follow the same stipulations for all HIPAA privacy and security regulations as the CE. However, depending on the agreement, they may have additional regulations, such as those with the FTC.
- Examples of organizations that typically have BAAs with healthcare providers:
  - ✓ Accountants, Lawyers, Collection Agencies, and Billing Companies

Having a Business Associates Agreement in place offers assurances that privacy and security standards are met.

UB|MD
PHYSICIANS' GROUP

Using Cellphones

Reminder:

Keeping patient information or images on your private cell phone for UBMD is **NOT** allowed.

- You may be held personally liable for fines if the confidentiality of the patient is violated and breached.

Only secured text messaging is allowed with a secured text message that is encrypted and authorized by UBMD.

UB|MD
PHYSICIANS' GROUP

HIPAA and UBMD Email

UBMD Email Reminder:

DO:

ONLY SEND PATIENT INFORMATION VIA SECURED FORMAT IN A ZIX MESSAGE OR ANOTHER APPROVED UBMD SECURED FORMAT

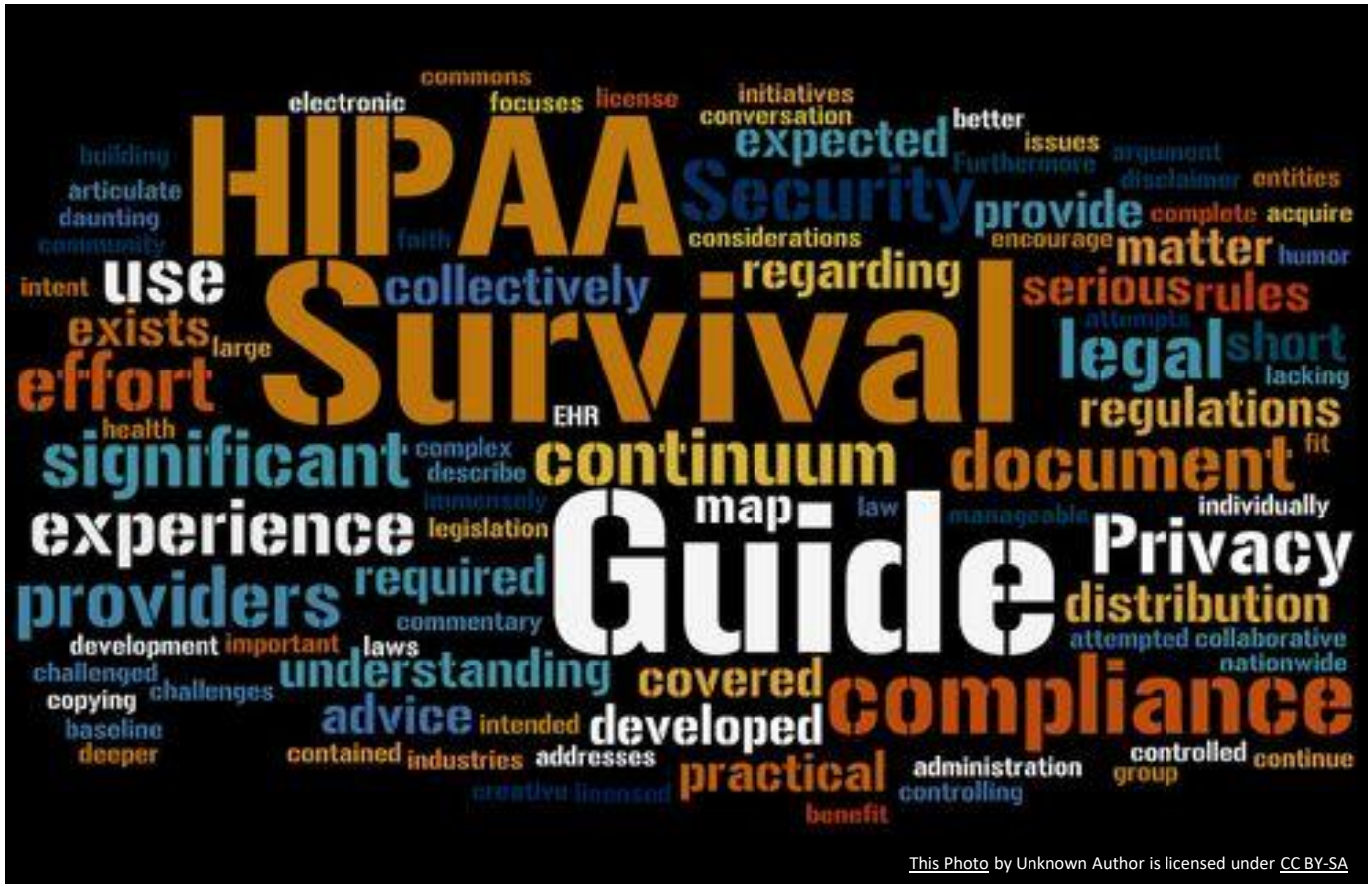
1. **Do NOT** include private health information for patients in your unencrypted emails.

2. **Do NOT** put patient information in the subject line of the email. Including:
   - Name/DOB
   - Medical Record Number
   - Account Number

3. **Do NOT** send images that can identify a patient by email.

UB|MD
PHYSICIANS' GROUP

HIPAA- The Good and The Bad



UB|MD
PHYSICIANS' GROUP

HIPAA Good Habits

- Establish STRONG passwords for your log-ins.
- Do not leave Post-it notes with the passwords viewable for easy access for others to see - secure them.
- Do not share your passwords; HIPAA is not a free streaming service.
- Control+ALT+Delete to lock your computer screen whenever you're away from your seat, even for a minute. This will prevent someone else from logging onto your system without a password.
- Be aware if someone remotes into your computer. Did you ask for technical assistance from OMC, for example?
- Be cautious of spam and phishing emails - you will get these!
- Be aware of suspicious emails or attachments - bad actors are very tricky and can make you act urgently to open your email and attachments!

UB|MD
PHYSICIANS' GROUP

Risky HIPAA Habits

- Do not search or look at your **own** medical records or for friends, family, co-workers, and VIP's health information. Speak to the Compliance Office for further questions on this topic.
- Do not post patient's private health information on social media.
- Do not text or email private health information UNLESS:
  - You need to Text/Email as it relates to your job function and treatment, payment, and operations (TPO). Make sure it is in a secured and encrypted platform.
  - Follow the Minimum Necessary Rule as it pertains to the access necessary to perform the needed functions of your job and patient care.
  - Patient requests transmittal of unencrypted PHI and we respond to that email.
- Avoid downloading malicious files and searching websites that are not secure.
- Not appropriately disposing of private health information. Make sure you use the correct and secured disposal bins.

UB|MD
PHYSICIANS' GROUP

Risky HIPAA Habits - Continued

- Make sure you are speaking in low tones and discreetly about a patient's health information. Do not speak in public areas such as an elevator, restrooms, cafeterias, or hallways.
- Be aware of what information you are leaving on voicemails, whether it be on an answering machine or voicemail system such as on a cell phone. Leave the minimum information necessary.
  - HHS guidance is as follows: A covered entity (CE) might want to consider leaving only its name and number and other information necessary to confirm an appointment or ask the individual to call back. Do not leave details.
- Do not leave medical charts available and accessible to unauthorized personnel. Secure the information if you are not at your desk or workstation.
- Do not leave patient information on scanners or fax machines for extended periods of time. Make sure you check that periodically and secure the information to the appropriate intended source.

UB|MD
PHYSICIANS' GROUP

Risky HIPAA Habits - Continued

- Do not respond to online negative reviews regarding patient information or treatment. Instead, ask the reviewer to contact the office to discuss this further. If it is a positive review, thank them for their positive feedback and experience with UBMD.

When in doubt:

Please contact the
Compliance Office to ensure
HIPAA Privacy Compliance.

UB|MD
PHYSICIANS' GROUP

Reporting HIPAA Violations

As healthcare workers and UBMD employees, you are **obligated** to immediately report any **known or suspected** violations of HIPAA or any other misconduct, violations of law, acts of retaliation, or other wrongdoing.

Reports may be made in any the following ways:

- Report directly to a practice plan supervisor.
- Report directly to the UBMD Chief Compliance Officer.
- Call the anonymous Compliance Hotline at 716.888.4752.
- Complete a Compliance Issue Reporting Form, which is available via our UBMD Compliance Office website. (https://www.ubmd.com/about-ubmd/Compliance/Compliance-hotline-reporting.html)

A report of misconduct alone does not automatically lead to the discipline of the subject of the report. For this reason, employees are encouraged to contact the UBMD Compliance Office to discuss or report situations, even if the reporting individual is not certain that the situation in question rises to the level of noncompliance.

UBMD's non-retaliation policy will always be strictly adhered to.

UB|MD
PHYSICIANS' GROUP

UBMD Compliance Hotline

UBMD COMPLIANCE HOTLINE: 716.888.4752

The Compliance Hotline is a non-traceable voicemail box, regularly monitored during business hours. When calling the Hotline, you may remain anonymous if you wish, but it is necessary that you provide all relevant information to the incident being reported:

- Practice Plan/Department;
- Date(s) & time(s) of incident(s);
- Detailed description of the incident or behavior in question;
- Name(s) of the person in question;
- Any other pertinent information.

*Since the hotline is **not** monitored 24/7, if **there is an immediate threat to person or property involved**, please DO NOT leave a message. Contact your direct supervisor immediately!*

UBMD's non-retaliation policy will always be strictly adhered to.

UB|MD
PHYSICIANS' GROUP

HIPAA Case Examples

UB|MD
PHYSICIANS' GROUP

HIPAA Examples

Case 1:

You are reviewing a chart for coding and billing. You notice the patient is a Buffalo Bills player who has received services at a UBMD practice. You are excited to read about one of your favorite players. At lunch, you can't wait to tell your co-worker that you have the "scoop" on what is really happening with the player for next week's game.

Is this a HIPAA violation?

If this is a HIPAA violation, how is this a HIPAA violation?

UB|MD
PHYSICIANS' GROUP

Case Example #1 Breakdown

Is this a HIPAA Violation?

Yes, this is a HIPAA violation; disclosing patient information is a HIPAA violation without the purpose of treatment, payment, or operational means.

How is this a HIPAA violation?

The co-worker does not need any of this information about the celebrity sports player to perform their job. This was inappropriate. Under HIPAA, this is a privacy disclosure, and the patient's privacy was disclosed and violated.

Patients receiving medical care expect privacy, and they expect a level of privacy no matter who they are. They expect a level of interaction that will be respected, and their PHI will not be shared.

UB|MD
PHYSICIANS' GROUP

Case Example 2

Case Example 2:

You work for a UBMD practice, and a patient has requested their medical records. They have placed a request for their personal health information. The patient has filled out, signed, and paid for the necessary documentation. The patient has been waiting **over 30 days** for the information.

Is this a HIPAA Violation?

Yes. This falls under Patient Information Blocking. Patients have a right to their medical records in a reasonable time. Denying patients their medical records because they cannot pay for the copy fee or overcharging them for the copy fee is a direct violation of HIPAA. Typically, in NYS, access to medical records is within 10 days of the request.

There are exceptions to this rule; for example, if the physician feels the information in the records may harm the patient or others.

UB|MD
PHYSICIANS' GROUP

Resources

Further Information can be found at the following sites :

https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html

https://www.healthit.gov/sites/default/files/page2/2020-08/Health_Care_Provider_Definitions_v3.pdf

https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/

https://www.healthit.gov/topic/information-blocking

https://www.hipaajournal.com/hipaa-business-associate-agreement/

https://wnydocs.org/Release-of-Medical-Records#:~:text=Patient%20Access%20to%20Record&text=Although%20reasonable%20time%20is%20not,between%2010%20and%2014%20days.

UB|MD
PHYSICIANS' GROUP

UBMD Compliance Office

Lawrence DiGiulio, Esq., Chief Compliance Officer
larryd@buffalo.edu

Suzanne Marasi, Compliance Administrator
smmarasi@buffalo.edu

UB|MD
PHYSICIANS' GROUP

Telemedicine 2026

Updates Calendar Year 2026

Telehealth continues to be revised on a governmental and state level. Please check NGS Medicare, Local Payer and Commercial guidelines for the most current coding and reimbursement guidelines.

UB|MD
PHYSICIANS' GROUP

Telemedicine Key Points

- Documentation and Payment of Telehealth is payer-specific.
- UBMD follows Medicare guidelines and recommendations.
- Effective until December 31, 2027.
- Must be on a HIPAA-compliant software platform such as Doxy.

UB|MD
PHYSICIANS' GROUP

Audio/Visual Telehealth Documentation

Providers can choose either Time or MDM – To select the level of E/M Codes:

- Patient consent must be documented prior to rendering the service to the patient (written or verbal).
- Inform the patient of possible cost sharing, as the patient might have a patient cost responsibility.
- **MUST** be on audio on HIPAA-compliant software platform (for example: DOXY, Zoom for Healthcare).
- **Verify with Payers** whether they still endorse the utilization of E/M codes 99202-99205 and 99212- 99215 with Mod 95, or that you must now utilize the new Telemedicine codes published in 2025.

UB|MD
PHYSICIANS' GROUP

Audio/Visual Telehealth Documentation

Further Documentation Guidelines:

- The visit was initiated by the patient, who was present for the visit.
  - Patient requests/confirms Telehealth visit.
- Document patient location (i.e., home, office, clinic, etc.)
- Document provider location.
- Document the reason for the visit.
- Document as if this is an office visit.
- If using Time for your visit code, you must document how you spent that time with the patient.
  - Example: A total of 20 minutes was spent with Mr. Z today for his follow-up encounter. For this time, I reviewed the patient charts prior to the visit. During the visit, we discussed the plan regarding his HTN, HDL, and 2DM. Prescription management options were discussed and ordered. A follow-up is set for a 6-month visit. Please review my assessment and plan for further details.

Very Important: ***Document a description of how that time was accrued for the patient. This can be pre-, intra-, and post-time for a TOTAL time for the day of the appointment.****

UB|MD
PHYSICIANS' GROUP

Billing Notes

- Check with insurance companies as not all insurance companies will pay for Telehealth Audio Visits and Modifiers utilized for billing.
- Telehealth is not to be billed for the delivery of biopsy results, MRI results, blood work results, test results, etc.
- Telehealth cannot be billed if a visit is related to a previous E/M encounter within the past 7 days.
- Telehealth cannot be billed if related to preplanned E/M encounter within 24 hours.
- Telehealth cannot be billed if this service results in the scheduling of an E/M encounter within 24 hours.
- Home Address Location Site:
  - ✓ For providers, for 2026 this is now a permanent policy. Provider's home address may be suppressed, if necessary, not to show on the HCFA 1500 claim form IF providing Telehealth services.
- FYI: Mental and Behavioral Health have additional notes.

UB|MD
PHYSICIANS' GROUP

Synchronous Audio – Only Visits
DO NOT REPORT FOR MEDICARE PATIENTS

Evaluation and management service by a physician or other qualified healthcare professional. These are payer specific reimbursement codes. Medicare does not reimburse these codes. These new codes contain a 10 min medical discussion.

PAYER DEPENDENT ON FEE SCHEDULE

- **98015 -** Medically appropriate history and exam . HIGH MDM and more than 10 mins of medical discussion. When using TOTAL TIME. Time must be documented of **40 mins to meet or exceed.**
- **98014** - same as above - TOTAL TIME must be documented **30 mins to meet or exceed** with an appropriate MDM of Moderate
- **98013** - same as above - TOTAL TIME is 20 mins to meet or exceed with an appropriate MDM of LOW.
- **98012** - Medically appropriate history and exam. Straightforward decision making is utilized. When using TOTAL TIME, Time must be documented for 10 mins to be met or exceeded.

UB|MD
PHYSICIANS' GROUP

Synchronous Audio-Video E/M Services

Table 2: Telemedicine and Non-Face-to-Face Services

Service	New/Established	Synchronous	Level/Unit Reported	Service Reported	Other E/M Notations
Synchronous audio-video (98000-98007)	Both	Yes	MDM or total time on the date of the service. No minimum required time, unless level selected by time.	Per single calendar date	Do not report with same-day in-person E/M
Synchronous audio-only (98008-98015)	Both	Yes	MDM or total time on the date of the service. Must be more than 10 minutes of medical discussion.	Per single calendar date	Do not report with same-day in-person E/M
Brief synchronous communication technology service (98016) MCR pays this CPT	Established	Yes	A single 5- to 10-minute medical discussion	Per single calendar date	Not related to E/M in prior 7 days or leading to E/M in next 24 hours
Online digital E/M (99421-99423)	Established	No	Minutes during 7-day period	Per 7 days	Not related to E/M in prior 7 days or leading to E/M in next 24 hours
Interprofessional telephone/Internet/EHR consultations (99446-99451)	Both	Not required	Minutes during 7-day period	Per 7 days	No in-person encounter within 14 days
Interprofessional telephone/Internet/EHR consultations (99452)	Both	Not required	Minutes during a single day	Per 14 days	Do not report with same-day E/M
Care management and remote treatment management (99424, 99425, 99437, 99484, 99491)	Established	Not required	Minutes	Per calendar month	Physician or other QHP time excluded on date of other E/M
All services (98000-98016, 99421-99425, 99437, 99446-99452, 99484, 99491)	Same time is not counted twice				

CPT's 98000-98007 maybe reported for new or established patients. Synchronous audio and video telecommunication is required. These service maybe reported on the DOS by either MDM or TIME.

Table AMA/CPT ®

Payer Information

As of January 2026, Payer Information Telehealth

Telehealth Billing Guidelines – As of Jan 2026

Payers NOT accepting NEW Telehealth Codes:

Need to utilize Mod 95 Along with 99202-99205 or 99212-99215

- Medicare
- All Medicare Advantage Plans
- NYS Medicaid
- ALL Medicaid based plans (i.e., Fidelis, IHA Medisource, Univera Safety Net plans, Molina, Amerigroup BMMC, etc.)
- Commercial UHC & BCBS plans are **not** accepting new Telehealth
- If only audio was used, the provider must document the reason, and we need to add modifier 93 to the E/M.

Payers that are accepting the new Telehealth codes:

- IHA - commercial
- Univera - commercial
- Aetna - commercial

UB|MD PHYSICIANS' GROUP

Summary

The Consolidated Appropriations Act, 2026, H.R. 7148, that was signed into law on February 3, 2026:

- Extends critical Medicare telehealth flexibilities through December 31, 2027.
- Preserves home-based telehealth access for Medicare beneficiaries.
- Removes long-standing geographic restrictions for telehealth services.
- Maintains Medicare coverage for audio-only telehealth services.
- Continues authorization for RHCs and FQHCs to serve as a distant-site telehealth providers.
- Extends the Acute Hospital Care at Home waiver program through 2030.

Overall, the bill provides regulatory stability and ensures continued access to virtual care for Medicare beneficiaries. It includes stability for Medicare telehealth services through 2027, preserving broad access to virtual care, maintaining coverage for home-based and audio-only services, and supporting rural and underserved communities.

UB|MD
PHYSICIANS' GROUP

Resources

CMS Telehealth-faq-updated-11-26-2025.pdf

https://telehealth.hhs.gov/providers/telehealth-policy/telehealth-policy-updates

https://www.medicare.gov/coverage/telehealth

UB|MD
PHYSICIANS' GROUP

Compliance Department

Larry DiGiulio, General Counsel and Chief Compliance Officer
Suzanne Marasi, Legal and Compliance Administrator

UB|MD
PHYSICIANS' GROUP

Cultural Competency Training: Instructions & Links

PHYSICIANS, NURSE PRACTIONERS & PHYSICIAN ASSISTANTS: Please complete the course titled "A PHYSICIAN'S PRACTICAL GUIDE TO CULTURALLY COMPETENT CARE" and save your completion certificate in case you are asked to show proof of completion. Your Human Resources department or other practice representative may ask you to send certificates to them.

- Three courses are available to choose from (**you only have to complete one course per year**). Providers can alternate year-to-year between the various courses.
- If you have taken the program in its entirety and need to retake the program, request an email reset by emailing: contact@thinkculturalhealth.hhs.gov or calling: 833-485-1664·

Please use this link for the physician/nurse practitioner course:
https://thinkculturalhealth.hhs.gov/education/physicians

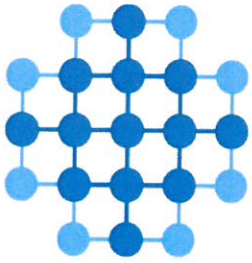
◊◊◊◊◊◊◊◊◊◊◊◊

ADMINISTRATIVE & CLINICAL STAFF: Please complete the course titled "GUIDE TO PROVIDING EFFECTIVE COMMUNICATION AND LANGUAGE ASSISTANCE SERVICES".

This course will NOT grant you a certificate of completion. Instead, by taking our training quiz, you are attesting to completing all training, including the Cultural Competency Training course.

Please use this link for the administrative/clinical staff course:
https://thinkculturalhealth.hhs.gov/education/communication-guide

Think Cultural Health can determine whether or not someone actually completed the program (should it come up during a state or federal investigation of a practice plan in the future), so it is strongly advised that no one sign the Attestation of Completion without actually doing the training.



UB|MD

PHYSICIANS' GROUP

UBMD Compliance Plan

2020

TABLE OF CONTENTS

ATTACHMENTS

I. INTRODUCTION

The FPMP Governing Board, UBA Executive Committee, and affiliated university faculty practice corporations (collectively, "UBMD") is committed to the very highest standards of ethics and integrity. The environment in which we deliver health care continues to rapidly evolve and become increasingly complex. As such, we have developed this Compliance Plan in an effort to assist our employees to conduct themselves in a manner consistent with the spirit and the letter of the laws, rules, and regulations that apply to this very highly regulated environment. All of our employees are strongly encouraged to use this Compliance Plan as a tool to guide them in the activities and services they perform each day on behalf of UBMD.

The FPMP Governing Board and UBA Executive Committee fully endorse this Compliance Plan and support the efforts of all of our employees as they continue to promote a culture of compliance and ethics.

Anne Curtis, M.D.
President, UBA Executive Committee
Approved by UBA Executive Committee

Dori Marshall, M.D.
President, FPMP Governing Board
Approved by Governing Board

II. UBMD AFFILIATED UNIVERSITY FACULTY PRACTICE CORPORATIONS

University at Buffalo Anesthesiology, Inc.
UBMD Dermatology, Inc.
University Emergency Medical Services, Inc.
UB Family Medicine, Inc.
University Gynecologists & Obstetricians, Inc.
Academic Medicine Services, Inc.
University Neurology, Inc.
University at Buffalo Neurosurgery, Inc.
University Nuclear Medicine, Inc.
University Ophthalmology Services, Inc.
University Orthopaedic Services, Inc.
University at Buffalo Otolaryngology, Inc.
University at Buffalo Pathology, Inc.
University at Buffalo Pediatric Associates, Inc.
University Psychiatric Practice, Inc.
University Radiology at Buffalo, Inc.
University at Buffalo Surgeons, Inc.
University Urology, Inc.

UBMD COMPLIANCE PROGRAM STAFF

UBMD General Counsel & Chief Compliance Officer
Lawrence C. DiGiulio, Esq.
UB Downtown Gateway Building
77 Goodell Street, Suite 310
Buffalo, New York 14203
(716) 888-4705
larryd@buffalo.edu

UBMD Compliance Administrator
Suzanne M. Marasi, CHC, CPCA
UB Downtown Gateway Building
77 Goodell Street, Suite 310
Buffalo, New York 14203
(716) 888-4708
smmarasi@buffalo.edu

UBMD Director of Audit & Education
Peter V. Rossow, CPC, CPMA
UB Downtown Gateway Building
77 Goodell Street, Suite 310
Buffalo, New York 14203
(716) 888-4702
pvrossow@buffalo.edu

III. ELEMENTS OF AN EFFECTIVE COMPLIANCE PLAN

The Department of Health and Human Services, Office of Inspector General ("OIG") has stated that every effective compliance program should begin with a formal commitment by the physician practice to address all of the applicable elements listed below, which are based on upon the seven steps of the Federal Sentencing Guidelines as well as the guidelines set forth by the New York State Office of Medicaid Inspector General:

A. Code of Conduct and Written Policies and Procedures

Compliance standards should be established through the development of a code of conduct and written policies and procedures. Such policies and procedures shall describe compliance expectations, implement the operation of the compliance program, provide guidance to employees and others on dealing with potential compliance issues, identify how to communicate compliance issues to appropriate compliance personnel and describe how potential compliance problems are investigated and resolved. The UBMD Code of Conduct is part of this Compliance Plan. Policies & Procedures are found in this Compliance Plan at UBMD and in each Practice Plan.

B. Designated Compliance Officer

An employee that is vested with responsibility for the day-to-day operation of the compliance program should be appointed. Such employee's duties may solely relate to compliance or may be combined with other duties so long as compliance responsibilities are satisfactorily carried out. Such employee shall report directly to the president or other senior administrator and shall periodically report directly to the Executive Committee and FPMP Governing Board on the activities of the compliance program. Lawrence C. DiGiulio, Esq. is the UBMD Compliance Officer.

C. Training & Education

All UBMD employees and applicable contractors, including executives and governing body members, shall be trained on compliance issues, expectations, and the compliance program operation. Such training shall occur annually and shall be made a part of the orientation for all new employees and governing board members. Appropriate training is provided to new and existing employees.

D. Internal Monitoring & Auditing

A system shall be in place for routine identification of compliance risk areas specific to UBMD, for self-evaluation of such risk areas, including internal audits, and, as appropriate, external audits, and for the evaluation of potential or actual non-compliance as a result of such self-evaluations and audits. Risk Assessments and audits are conducted on a regular basis.

E. Communication

Communication lines to the compliance officer shall be in place and accessible to all employees, persons associated with UBMD, executives and governing body members, to allow compliance issues to be reported. Such communication lines shall include a method for anonymous and confidential good faith reporting of potential compliance issues as they are identified. UBMD has an anonymous Compliance Hotline (888-4752), regular compliance meetings, quarterly newsletter and many other means of communication between employees and the Compliance Office.

F. Enforcement of Disciplinary Standards

Considerable effort has been made in the development of UBMD's Compliance Office, which is charged with the responsibility of responding to allegations of improper activities. The Code of Conduct (Part IV) and other Policies (Part V) within this Compliance Plan have been established to ensure UBMD employees are aware that Compliance shall be treated seriously, and that violations and non-compliance shall be dealt with fairly, consistently and uniformly.

G. Responding to Detected Violations

Reasonable and prompt steps shall be taken to respond to all violations detected through audits and monitoring, and those that are reported by individuals. Implementation of a corrective action plan shall take place for any violations confirmed by an investigation.

H. Non-retaliation

Retaliation for reporting compliance concerns in good faith will not be tolerated regardless of whether or not a violation is found as a result of the initial report. Reports of retaliation shall be investigated thoroughly, and can result in disciplinary action up to and including termination of employment.

This policy includes but is not limited to reporting potential issues, investigating issues, self-evaluations, audits and remedial actions, and reporting to appropriate officials as provided in sections 740 and 741of the New York State Labor Law (whistleblower provisions for health care fraud).

UBMD is committed to providing quality health care services in compliance with all applicable laws and regulations. This Code of Conduct is a statement of UBMD's dedication to upholding the ethical, professional and legal standards we use as a basis for our daily and long term decisions and actions.

A. Compliance with Laws, Regulations, Policies and Procedures

All UBMD employees must understand and comply with all relevant policies, laws and regulations, and are individually and collectively responsible and accountable for upholding these standards of compliance. Supervisors and Compliance Coordinators are responsible for teaching and monitoring compliance, with the guidance and oversight of the UBMD Compliance Office.

Each Practice Plan will designate an employee as their Compliance Coordinator. That person will remain in that position until replaced by another employee. The Compliance Coordinator may have other duties as well as his or her compliance duties.

B. Patient Referrals

Relationships with other providers must comply with all applicable laws. Patient referrals are to be made and accepted based on medical needs only. No UBMD employee should ever accept or offer any type of payment or compensation in exchange for patient referrals, patient consultations or the purchase of services to a hospital or other facility. Any such offers should immediately be reported to a supervisor, compliance coordinator, or the UBMD Compliance Officer.

C. Claims for Reimbursement

UBMD will only submit claims for reimbursement for services that were provided, documented in the medical record, and medically necessary. Reimbursement claims should never contain false or misleading information.

If an employee becomes aware of a situation in which a false claim has been made or submitted, that employee must report it immediately to a supervisor, compliance coordinator or the UBMD Compliance Officer.

It is a federal crime, in violation of the Federal False Claims Act, to knowingly submit false claims to Medicare, Medicaid or any health care benefit program. All billing activities, therefore, are subject to the federal criminal and civil sanctions, regardless of payer.

D. Confidential Information

Many UBMD employees have access to various forms of sensitive and confidential information in regards to patients and co-workers. Any and all confidential and Protected Health Information ("PHI") obtained either during the course of assigned duties or accidentally should not be released or discussed with anyone unless the individual is authorized to receive the information. UBMD prohibits the unauthorized seeking, disclosing or selling of such information. Thus,

employees should not seek access to confidential information out of curiosity, for malicious purposes or for financial gain.

UBMD employees are prohibited from accessing their own, coworker's, family member's or patient's PHI unless they have a clear requirement to do so, and then may only access the Minimum Necessary PHI as needed to perform their job.

E. Conflict of Interest

All UBMD employees are prohibited from engaging in any activity, practice or act of financial interest that conflicts with or appears to conflict with the interests of UBMD or any professional setting where the employee engages in the practice of medicine. A conflict of interest may occur if an employee's outside activities or personal interests influence or appear to influence his or her ability to make objective decisions on the job. A conflict of interest may also exist if the demands of outside activities hinder or distract the employee from the performance of his or her job or cause the employee to use UBMD resources for purposes not related to UBMD business. Therefore, employees should avoid any actions that might lead someone to believe there is a conflict of interest. Questions regarding conflicts of interest should be directed to a supervisor, compliance coordinator or the UBMD Compliance Officer.

In addition to this Conflict of Interest statement, UBMD has a Conflict of Interest Policy for its Officers, Directors and key employees. (See Attachment A)

F. Business Information and Relationships

1. Acceptance of Business Courtesies

UBMD employees may not solicit or accept gifts or payments that exceed $100 individual or $250 in total during one calendar year from individuals or business organizations with business intents, contracts or transactions with UBMD. Such action may appear to influence objectivity in performing our work, or give the appearance of providing personal gain or showing favoritism to an individual and/or current or potential business partner. Any gifts or payments must be reported to the UBMD Compliance Office within thirty days of its receipt. If a situation arises which conflicts with this policy, contact your supervisor or the UBMD Compliance Officer immediately.

2. Competitor Information

UBMD employees shall not obtain proprietary or confidential information about a competitor through illegal or unethical means. Information may be gathered about other organizations, including our competitors, through legal and ethical means, such as public documents and other published and spoken information.

3. Contract Negotiation

UBMD employees will comply with all applicable disclosure rules and regulations honestly and completely. Employees involved in the negotiation of a contract must ensure that all the data generated, supplied and represented is accurate, current and complete. Failure to follow these guidelines may result in civil or criminal liability for UBMD, the involved employee and any managers or supervisors who condone such a practice. UBMD employees shall not contract to obtain services or products from an individual or company that has been convicted of a criminal offense related to health care and/or is listed by a federal agency as debarred, excluded or otherwise ineligible for participation in federally funded health care programs.

G. Violations

Confirmed violations of this Code of Conduct will result in appropriate disciplinary action against the offending individual(s), up to and including termination from employment.

V. POLICIES

A. Education & Training

Government and third-party payer laws, rules and regulations are continuously changing. As such, an ongoing, effective education and training program is vital to the UBMD Compliance Plan, ensuring that all employees – faculty physicians, residents, and all staff members – have open communication with the UBMD Compliance Office, and a full understanding of the how the Compliance Plan and laws apply to them.

Understanding and adhering to the Compliance Plan will result in fewer possible compliance discrepancies, thus protecting UBMD from internal and external exposure. All employees are required to complete annual Compliance training to include HIPAA, Fraud, Waste & Abuse and Diversity.

Much of the UBMD Compliance training will be completed online, which requires entering an employee's UBIT Name. (The UBIT Name is the username used to log into various campus services.) It is, therefore, **required** that all new UBMD employees have a UBIT Name **prior** to beginning work. It is the hiring Practice Plan's responsibility to ensure that the required paperwork is completed and submitted as necessary to have UBIT Names assigned prior to commencement of employment.

1. Mandatory New Hire Training

Within six months of commencement of employment within UBMD, all new employees must attend a one-hour compliance orientation and training session with the UBMD Compliance Officer or his/her designee. This session will include a full review of the UBMD Compliance Plan, Medicare documentation and billing requirements, and an opportunity for questions and answers. All new employees must complete Attachment E of the Compliance Plan (Employee Acknowledgment) and return to their Human Resources department. Failure of a new employee to

attend this session may result in disciplinary action up to and including termination of employment.

2. Mandatory Annual Training

All UBMD providers and employees are required to complete a minimum of two (2) hours of compliance training biennially (every two years). This training may include, without limitation:

a. One-on-one educational sessions with your internal chart auditor;
b. Small group sessions with internal chart auditors, the UBMD Compliance Officer, or his or her designee;
c. Classes or seminars presented by the UBMD Compliance Office;
d. Documented review of the quarterly UBMD Compliance Newsletter and satisfactory completion of accompanying quiz (15 minutes of training credited per issue reviewed/successfully completed quiz);
e. Presentations made by outside consultants or medical billing specialists, subject to the approval of the UBMD Compliance Office;
f. Off-site conferences and/or seminars covering health care compliance topics, subject to the approval of the UBMD Compliance Office;
g. Computer-based compliance training programs; or
h. Personalized educational sessions provided by the Compliance Office, as needed or requested.

Each Practice Plan is responsible for maintaining documentation verifying physician and employee attendance at all applicable educational sessions, and for forwarding all such documentation to the UBMD Compliance Office for review, ensuring adherence to this policy.

3. Other Educational Services

The UBMD Compliance Office will distribute an electronic newsletter four (4) times each year. This newsletter will contain pertinent legal and compliance-related updates, information, advice and tips. All UBMD employees are strongly encouraged to read each newsletter and direct questions or ideas concerning the newsletter to the UBMD Compliance Office.

The UBMD Compliance Office also maintains a compliance website which is linked to the UBMD website (https://ubmd.com), in the dropdown menu under "About UBMD" – "Employees: Compliance Office". The website will include reference materials including but not limited to: a copy of the UBMD Compliance Plan, past newsletters, PowerPoint training programs, and general compliance topics. UBMD employees are encouraged to use this website as an ongoing compliance learning and reference tool.

The Compliance Officer is also available to provide personalized advice and to assist with day-to-day compliance related questions or concerns. He or she is qualified to address a wide range of compliance issues, and should be consulted whenever there is a need for compliance training or educational assistance. Consultations with the Compliance Officer in this regard may, in many instances, be credited toward a physician's or employee's 2-hour compliance education requirement.

The Director of Audit and Education is available to provide advice and educational assistance relating to documentation requirements, coding, and billing issues. Time spent in such training is applied to compliance educational requirements.

B. Coding & Documentation

1. Overview

Medical coding identifies and classifies health information used in a physician's billing process so that a physician's payment is optimized, but not maximized. Proper documentation facilitates quality care and verifies the services that were provided. Complete and accurate documentation regarding the diagnosis and treatment in a patient's medical record is imperative.

The medical record of a patient may be used to validate site of service, appropriateness of the services provided, the accuracy of the billing, and identity of the health care provider who furnished the services.

All medical records generated by all UBMD physicians must be complete and legible, and include the following elements:

- Reason for the encounter/chief complaint
- Relevant patient history
- Physical examination findings
- Prior diagnostic test results
- Assessment, clinical impression or diagnosis
- Plan for care
- Date and legible identity of the observer
- Statement of rationale for ordering diagnostic tests and other ancillary services, if not documented and easily inferred by a third party reviewer with appropriate medical training
- Past and present diagnoses accessible to the treating and/or consulting physician
- Identification of appropriate health risk factors
- Statements of patient's progress, response to and changes in treatment, and revision of diagnosis
- Addendums to the medical record should be dated the day the information is added to the record and not for the date the service was provided.

CPT-4 and ICD-10-CM codes reported on all reimbursement claim forms or billing statements should be adequately supported by the documentation in the medical record, and be submitted only in the name of the provider who performed the service.

While the above principles of documentation are applicable to all UBMD providers, it is the responsibility of the individual Practice Plans to implement any documentation guidelines specific to the nature and type of service they provide. The Practice Plans are responsible for orienting all of their employees – clinicians, coders, billers, administrative staff and auditors – to the documentation

guidelines. Practice Plans may ask UBMD Compliance Office for assistance with this training.

2. PATH Requirements

Payment for teaching physicians provided in teaching settings using physician fee schedule is permissible only if:

- Services are personally provided by physician, not resident;
- Teaching physician is physically present during key portions of the service that resident performs; or
- Teaching physician provides care under conditions outlined in "documentation" paragraph in Part V, Section B-1 of this Compliance Plan.

For purposes of payment, E/M services billed by the teaching physician require that they personally document at least the following:

- Review of resident's note;
- Confirm or edit of resident's findings;
- Document performance or participation in key components;
- Summarize participation in the management of the patient; and
- Date, time, and signature on note.

Examples of correct wording:

- "I performed a history and physical examination of the patient and discussed his management with the resident. I reviewed the resident's note and agree with the documented findings and plan of care."
- "See resident's note for details. I saw and evaluated the patient and agree with the resident's findings and plans as written."

Examples of unacceptable documentation:

- "Agree with above."
- "Rounded, reviewed, agree."
- "Discussed with resident. Agree."
- "Patient seen and evaluated."

Primary Care Exception – A graduate medical education program that has been granted a primary care exception may bill Medicare for lower and mid-level E/M services provided by residents.

- E/M codes new patient: 99201, 99202, 99203;
- E/M codes established patient: 99211, 99212, 99213;
- HCPCS Code G0402: Initial preventive physical examination; face-to-face visit services limited to new beneficiary during the first12 months of Medicare enrollment;
- HCPCS Code G0438: Annual wellness visit, including personal preventive plan service, first visit;
- HCPCS Code G0439: Annual wellness visit, including personal preventive plan service, subsequent visit;

- CPT Codes 99381 – 99397: Preventive Medicine Services;
- Residents providing billable patient care service without teaching physician supervision must have completed at least six (6) months of GME program;
- Residency programs most likely to qualify for exception: family practice, general internal medicine, geriatric medicine, pediatrics, and obstetrics/gynecology.

3. Student Documentation of E/M Services

The teaching physician may verify in the medical record any student documentation of components of E/M services, rather than re-documenting the work. This is important for teaching physicians and those who provide coding services to teaching physicians.

Change Request 10412 which revises Chapter 12, Section 100.1.1 of the Medicare Claims Processing Manual states the following specifics regarding this:

- Students may document services in the medical record.
- The teaching physician must verify in the medical record all student documentation or findings, including history, physical exam and/or medical decision making.
- The teaching physician must personally perform (or re-perform) the physical exam and medical decision making activities of the E/M service being billed, but may verify any student documentation of them in the medical record, rather than re-documenting this work.

It is important that there is no question that the teaching physician verified the student's documentation and personally performed the physical examination and medical decision-making of the E/M service.

To ensure that we compliantly bill for these services, the following Student Attestation must be added and signed by the supervising physician:

> *"I have seen, personally examined and assessed the patient to establish a plan of care. I have reviewed the medical record and verify that all student documentation or findings, including history, physical exam and/or medical decision making are accurate. I have performed or re-performed, the physical exam and medical decision making activities to the extent they were conducted by a student."*

4. Non-Physician Practitioners

There are three (3) ways to bill for the services of non-physician practitioners ("NPP"):

a. **Incident-to services** are billed under the M.D., paid at 100% of the M.D. fee schedule.

   - Private office, outpatient only. No hospital outpatients, inpatients, emergency department patients.
   - Follow-up/established patients only. No new patients.
   - Requires "direct supervision" by physician.

- "Direct supervision" means the doctor must be present in the office suite, immediately available to provide service if needed.
- NPP documents service in medical record; M.D. does not need to sign.

b. **Direct billing** is billed under the NPP, paid at 85% of the M.D. fee schedule.

- Not site-restricted; may be inpatient, outpatient, office, hospital, etc.
- New or follow-up/established patient.
- Requires "general supervision" by M.D.
- "General supervision" includes the attending physician's overall direction and control of the training and equipment, but the physician's presence is not required during the diagnostic procedure. The physician does not have to be present when the service is performed.

c. **Shared billing** applies when NPP and M.D. are members of the same group, and the combined service is billed either under the NPP's or M.D.'s number.

- Not site-restricted; may be inpatient, outpatient, office, hospital, etc.
- E/M services only.
- No critical care, no SNG, no procedures, no consultations.
- M.S. must provide face-to-face portion of the E/M encounter.
- If incident-to requirements are not met, then must bill under the NPP's number. Local health insurers have adopted this as their "incident to" policy. Medicare has a separate policy that should be followed for Medicare patients.

d. **Scribes** are allowed by UBMD to be used by teaching/attending physicians. Residents, interns and fellows may not act as scribes. Ancillary providers such as NPs, PAs, MAs, RNs and other staff may serve as scribes. Medical students may act as scribes recording the actions and words of the physician in real time. Medical students must not be seeing the patient in any clinical capacity and may not document or interject their own observations or impressions. Do not confuse this ability to scribe with the medical student's ability to individually document information for a billable service.

Anyone acting as a scribe must receive appropriate compliance and computer training, review the UBMD policy on the Use of Scribes Policy and sign an agreement to adhere to the policy.

A scribed note must accurately reflect the services provided for any given date of services. The billing provider is responsible for the content of the scribed note.

A scribed note can be hand-written and scanned or typed/created directly in the EMR.

Documentation of a scribed service must include the following:

- A dated note from the scribe identifying them as the scribe for (name of the physician providing the service), attesting that the notes were written in the presence of the physician, and the signature of the billing physician.
- Individuals can only create a note in the EMR if they have password/access to the EMR. Documents scribed in the EMR must clearly identify the scribe and their authorship of the note both in the document and in the audit trail.
- Providers are required to document in compliance with all federal, state and local laws, as well as with UBMD policy.

A Scribe Agreement (Attachment B) should be completed by anyone acting as a scribe and returned to practice plan.

C. Electronic Medical Records

1. The Medical Record

A medical record is created for every patient who receives treatment, care, or services and is maintained for the primary purpose of providing patient care. The record should contain sufficient information to: identify the patient, support the diagnosis(es), justify treatment and facilitate the continuity of patient care. Any electronic medical record system used must comply with all HIPAA privacy and security requirements.

a. **Providers are prohibited from allowing others to use their password or sign their notes.** Providers are responsible for the total content of their documentation and that of residents, medical students or any other ancillary personnel under their supervision whether the content is original, copied, pasted, imported or reused.

b. **The record should clearly identify the author and date of all entries.** Entries must be signed/authenticated by the author. Electronic signatures must be password protected and used only by the author. All entries should be signed promptly, allowing a short delay that occurs in the transcription process.

c. **Providers documenting in the EHR must avoid indiscriminately copying and pasting progress notes and duplicate/redundant information provided in other parts of the EHR.** If any information is copied or reused from a prior note, the provider is responsible for its accuracy and medical necessity. The primary purpose of progress notes is to provide an accurate depiction of unique treatment rendered a specific date of service. Further requirements pertaining to copying and pasting progress notes:

   i. Copied information must be reconfirmed and revised as necessary to accurately reflect the specific date of service.

ii. It is not advisable to duplicate information that does not specifically impact a specific date of service.
iii. Copying of subjective data (i.e. history of present illness and plan of care) is strongly discouraged.
iv. Copying teaching physician attestations from previous notes is prohibited.
v. Information that is copied should not exceed six (6) months from the date of the original note.
vi. Information copied forward from the providers' original notes should be closely examined for accuracy, completeness and relevance.
vii. Documentation must reference the date of the original note. *Example*: "Copied from my previous note dated..."

d. **Providers are responsible** for citing and summarizing applicable lab data, pathology, and radiology reports rather than copy such reports in their entirety in the notes.

e. **Providers are responsible** for correcting any errors identified within their own document, via a dated amendment if the note is already signed.

f. **Providers are required** to document in compliance with all federal, state and local laws, as well as with UBMD policy.

2. Templates

Per CMS Transmittal 455, dated March 15, 2013, use of templates is not prohibited to facilitate recordkeeping, but CMS also does not endorse or approve any particular templates. Providers may choose any template to assist in documenting medical information. However, CMS does discourage the use of templates which provide limited options such as "check boxes" or predefined answers, and/or limited space to enter information, or those designed to gather selected information focused primarily for reimbursement purposes as they often fail to capture sufficient detailed clinical information to demonstrate that all coverage and coding requirements are met, or adequately show that medical necessity criteria for the service are met.

If using a template, UBMD providers are advised to select one that allows for a full and complete collection of information to demonstrate that the applicable coverage and coding criteria, as well as medical necessity, are met.

3. Cloning

Documentation is considered cloned when it is worded exactly like, or similar to, previous entries. It can also occur when the documentation is exactly the same from patient to patient. Individualized patient notes for each patient encounter are required. Documentation must reflect the patient condition necessitating treatment, the treatment rendered and, if applicable, the overall progress of the patient to demonstrate medical necessity.

4. EHR Audits

Electronic Health Records should be audited at the practice plan level by each practice plan on a quarterly basis as follows:

a. Review records of VIP patients to make sure records were accessed only by those who took part in the care and treatment of the patient.
b. Review records of UBMD employees who are also practice plan patients to make sure records were accessed only by those who took part in the care and treatment of the patient.
c. Randomly select up to five (5) practice plan employees, and check one day from the previous quarter to make sure their access to records were appropriate.

Any employee found to be inappropriately accessing the EHR of a patient will face disciplinary action up to and including termination.

D. Record Retention

Patient records and documentation must be retained according to any federal, state or local laws and regulations, and maintained for a sufficient period of time to ensure availability to prove compliance with laws and regulations.

All UBMD employees shall ensure that patient health information is available to meet the needs of continued care, legal requirements, research, education and other legitimate uses.

The following record retention guidelines shall be followed by all UBMD employees to meet the needs of our patients, providers, researchers, and other legitimate users, and complies with legal, regulatory and accreditation requirements.

- For adults, clinical records must be maintained for a minimum of seven (7) years from the last contact with the patient.
- For minors and obstetrics, clinical records must be maintained through the age of twenty-one (21) of the child, or seven (7) years from the last date of service, whichever is longer.
- Patient billing records must be maintained for seven (7) years. This includes maintenance of superbills, inpatient/outpatient/surgery charge cards, cash and credit card payment logs and copies of checks. Paper superbills that are added electronically do not need to be maintained.
- For deceased patients, clinical records must be maintained a minimum of 6 years after death.
- The record's retention requirement should be measured from the date of the last professional contact with the patient to determine the length of time the record is required to be retained.
- An electronic scan of the entire paper record will meet the retention requirement, provided the technology to access the record is maintained for the applicable period of time.
- In the event a patient files a lawsuit against UBMD, records should be maintained until the lawsuit is resolved.

- Under the False Claims Act, claims may be brought up to six (6) years after the incident; however, on occasion, the time has been extended to ten (10) years.

E. Audit & Monitoring

An ongoing audit program to monitor compliance with applicable laws and policies is integral to the UBMD Compliance Plan. The focus of UBMD's audit program is to assess the accuracy of documentation and coding of UBMD providers. The objectives of UBMD's accuracy monitoring are:

- To ensure accurate, complete and legible documentation of medical services provided;
- To ensure proper coding and billing based on the documentation;
- To determine whether or not any problem areas exist in documentation, coding or billing; and if so, to focus on improving those areas with the physician.

Routine prospective chart review is required for each Practice Plan to assess compliance with the established standards of practice and billing guidelines. Charts will be audited without regard to payer type. There are several types of audits that may be performed, including:

1. **Periodic Audits –** Designed to identify deficiencies and inconsistencies in the documentation and billing process in order to develop strategies for improvement, including educational sessions. The internal auditor for each Practice Plan will be responsible for annually reviewing the lesser of 2% of each provider's submitted claims, or 10 claims, unless a more stringent requirement is otherwise specified in the individual Practice Plan compliance policies.

   If a provider's charts are found to be less than 85% compliant, the internal auditor will conduct an individual educational session and perform a follow-up audit within six weeks to evaluate the effectiveness of the education. The provider will then receive a second, problem-focused, audit. Failure to improve compliance percentages may result in additional corrective action being taken as outlined in Part V, Section P of this Compliance Plan.

2. **Investigational Audits –** Conducted by an internal auditor, UBMD's Compliance Officer, or his/her designee in response to issues or concerns that might arise within a Practice Plan either by an employee or an outside source. The auditor will consult with the Compliance Officer or his/her designee and the Practice Plan President prior to conducting an unscheduled audit. For further information on internal investigations, see Part V, Section O of this Compliance Plan.

3. **Parallel Audits –** May be conducted any time an outside agency such as the U.S. Attorney's Office, U.S. Department of Justice or the New York State Attorney General's Office initiates an investigation of a UBMD provider or Practice Plan. These audits are intended to provide the UBMD Compliance Officer with information that may be helpful in defending or

settling any charges that may arise from the outside investigation. For further information regarding governmental investigations, see Part V, Section R of this Compliance Plan.

4. **Requested Audits –** Audits may be conducted at the request of the Compliance Officer at any time to ensure compliance with third party billing requirements and/or applicable fraud and abuse laws.

For the purposes of periodic audits, a minimum of ten (10) records will be reviewed annually per full-time provider. Each Practice Plan shall be responsible for reporting internal audit results to the UBMD Director of Audit & Education once each year, with a minimum of ten (10) records per provider. The audit reports shall be submitted on a form acceptable to the UBMD Director of Audit & Education once per year, as scheduled by the UBMD Director of Audit & Education. Audit results will contain information such as number of encounters reviewed, the number of compliant and noncompliant records, review codes for noncompliance, and follow-up activities for tracking and educational purposes. A plan of correction should be reported for all deficiencies identified.

Additional records may be reviewed at the discretion of the UBMD Compliance Officer.

Periodic and follow-up audits will be conducted by auditors retained by the individual practice plans. **In the event a Practice Plan does not retain an auditor, or if the auditor designated by the Practice Plan fails to review a minimum of ten (10) records per year per provider, then the Compliance Officer may choose to hire an auditor to fulfill such obligation, at the expense of the Practice Plan in question.**

Periodic audits are independent and impartial chart reviews. They shall remain separate from the coding function within the Practice Plan. **Auditors shall not be the same person who codes the medical records.**

F. Overpayments

Medicare Parts A & B health care providers are required to report and return overpayments to the appropriate party (i) by the later of 60 days after the overpayment was identified, or (ii) by the date the corresponding cost report is due, if applicable.

Health care providers who fail to report and return an overpayment face potential penalties including false claims liability, civil monetary penalties and exclusion from federal health care programs.

Overpayments must be reported only if a person identifies the overpayment within six years of the date that the overpayment was received. The six year look-back period will apply to any overpayments reported or repaid on or after March 13, 2016.

Any information or a potential overpayment shall be promptly evaluated for credibility, documented and followed up on accordingly. All Practice Plan providers and their staff are to use reasonable diligence to identify, report and

repay any overpayments using applicable claims adjustment, credit balance, self-reported refund, or other appropriate process established by the applicable Medicare contractor to satisfy the obligation to report and return overpayments.

G. Monitoring Exclusionary Databases

This policy applies to all UBMD practice plans who bill government programs including, without limitation, Medicare and Medicaid. Federal and state governments require healthcare providers to check the names of all providers, staff and agents/vendors against exclusionary databases. It is required that each UBMD practice plan check the following exclusionary databases ("Exclusionary Databases") according the time frames listed below:

1. U.S. Office of Inspector General's List of Excluded Individuals and Entities ("OIG-LEIE")
2. U.S. General Services Administration's System for Award Management ("GSA-SAM") (Formerly known as the Excluded Parties List System)
3. New York State Office of the Medicaid Inspector General List of Restricted and Excluded Providers ("OMIG List")
4. U.S. Treasury's Office of Foreign Assets Control Specially Designated Nationals ("SDN List")
5. U.S. Centers for Medicare and Medicaid Services National Plan and Provider Enumeration System ("NPPES")
6. U.S. Social Security Death Master File ("Death Master").

The following Exclusionary Databases **must be checked monthly**:

- OIG-LEIE
- GSA-SAM
- OMIG List

The following Exclusionary Databases must be checked against providers only **when a provider is credentialed or re-credentialed**:

- SDN List
- NPPES
- Death Master

If a match is found on any exclusionary database, the provider, staff member or agent/vendor should be immediately suspended. That person should be given the opportunity to appeal to the appropriate government agency to have his or her name removed from the Exclusionary Database or receive a waiver from the appropriate government agency.

If those actions are not successful, provider or staff member must be terminated from employment and the contract with the agent/vendor must be terminated.

H. Reporting Misconduct

It is the responsibility and duty of all UBMD employees to immediately report any known or suspected misconduct, violations of law, acts of retaliation, or other wrongdoing, either to the UBMD Compliance Officer or to a supervisor or manager with the respective Practice Plan.

1. Examples of Misconduct

- repeated instances of improper coding
- inadequate medical record documentation
- falsification or alteration of medical records
- harassment, intimidation
- threatening, vulgar or obscene behavior
- acceptance of bribes or other kickbacks
- unlawful attempts to induce referrals
- retaliation against someone who has made a previous report concerning a compliance violation
- HIPAA violations

2. Procedure for Reporting Misconduct

All reports of known or suspected misconduct may be made in any of the following ways:

- Report directly to Practice Plan President or Compliance Coordinator.
- Report to UBMD Compliance Officer via:
  - ✓ Phone: 888-4705
  - ✓ Email: larryd@buffalo.edu
  - ✓ Interoffice mail: Lawrence C. DiGiulio, 77 Goodell, Suite 310
  - ✓ U.S. Mail: Lawrence C. DiGiulio, 77 Goodell Street, Suite 310 Buffalo, New York, 14203
- Call the Anonymous Compliance Hotline at 888-4752.
- Complete a Compliance Issue Reporting Form.

A report of misconduct alone does not automatically lead to the discipline of the subject of the report. For this reason, employees are encouraged to contact the UBMD Compliance Office to discuss or report situations even if the reporting individual is not certain that the situation in question rises to the level of noncompliance.

All reports of misconduct should include pertinent information including:

- The name of the individual and/or Practice Plan about which the report is being made;
- A factual and objective description of the questionable practice, including date and time;
- If involving inappropriate billing, any information available regarding if/when claim was billed, amount billed, whether payment

was received, what steps if any were taken to stop payment or refund payment;
- Medical records involved, identified by either patient name or number;
- Any other information deemed necessary for investigation.

Each report of misconduct will be followed up with an internal investigation in accordance with Part V, Section O of this Compliance Plan. If warranted following a complete investigation, corrective action may be imposed in accordance with Part V, Section P of this Compliance Plan.

Confidentiality of employee reports will be maintained at all times, to the extent practicable and legal. Only those personnel who have a need to know will be informed of the reports.

3. Compliance Hotline

The Compliance Office will maintain a Compliance Hotline to create an open line of communication with UBMD employees. The normal hours of operation are Monday-Friday, 8:00am-5:00pm. However, the hotline will be accessible 24 hours, 7 days a week, allowing callers to leave a message no matter when they call.

A copy of the Compliance Hotline flier should be posted in all practice plan back-office areas, visible to employees. (Attachment C)

All calls to the hotline will be confidential, and no attempt will be made to determine the number or location of the caller. It is our policy to preserve anonymity of callers who wish to remain anonymous, subject to limits imposed by law.

4. Compliance Issue Reporting Form

The Compliance Office offers a Compliance Issue Reporting Form as another option for reporting misconduct. Once completed, the form may be sent to the Compliance Office via email, fax, US Mail. The form allows the reporter to remain anonymous if desired. (Attachment D)

Failure or refusal to report misconduct or fraudulent or illegal practices is a violation of this Compliance Plan and may result in disciplinary action, up to and including termination, of any individual who suspects misconduct but fails to report it.

I. Diversity

UBMD encourages and promotes diversity in its organization at all levels, and values individual and cultural differences within its workforce. UBMD is committed to an inclusive work environment, where everyone is treated with fairness, dignity and respect.

In support of this commitment, UBMD prohibits any conduct of discrimination against employees, patients, residents, fellows, students or vendors with regard

to race, color, religion, sex, national origin, age, disability, sexual orientation, marital status, pregnancy, military status, veteran status, or any other status or classification protected by federal, state or local law. Discrimination or harassment based on any protected status or classification will not be tolerated, and may result in disciplinary action up to and including termination.

J. Language Access Services

All UBMD practice plans will take reasonable steps to ensure that persons with Limited English Proficiency (LEP) and persons who are hearing impaired have meaningful access and an equal opportunity to participate in our healthcare services.

When necessary, each practice plan will provide interpretive services to LEP and hearing impaired patients.

Interpretive services will be provided by the practice plan through use of competent bilingual staff, staff interpreters, contracts or formal arrangements with local organizations providing interpretation or translation services, or technology and telephonic interpretive services. This assistance will be provided by the practice plan at no cost to the patient.

Each practice plan will inform LEP and hearing impaired persons of the availability of interpretive services, free of charge, by providing written notice in languages LEP persons will understand. Notices and signs must be posted and provided in reception areas and other points of entry.

A copy of New York State's Language Identification Tool, which may be used by practice plans, is included at the end of this Compliance Plan (Attachment F).

K. Social Media

Social media and social networking are internet communication sites on which users interact, and post or share information or content of any sort, whether or not associated or affiliated with UBMD, including but not limited to:

- Networking sites (ie: Facebook, LinkedIn)
- Messaging sites (ie: Twitter, Snapchat)
- Blogs, personal websites, forums, message boards, chat rooms, and the like
- Photo and video sharing sites (ie: Instagram, YouTube)

Personal use of social networking sites should be limited to non-work time, and should not interfere with your work or the mission of UBMD. Personal use of social media should not violate UBMD policies within this compliance plan in relation to co-workers, supervisors or other persons in the UBMD community. For example, social media should not be used to post comments or references to co-workers, supervisors or patients that are vulgar, harassing or threatening in nature, all of which are examples of misconduct according to the UBMD Compliance Plan.

UBMD employees should never post any information or rumors about the organization, other employees or patients that you know to be false, and should never represent oneself as a spokesperson for UBMD or make knowingly false representations about your credentials or your work at UBMD. If UBMD is a subject of the content you are creating, be clear about the fact that you are an employee, and make it clear that your views do not represent those of UBMD. It is best to include a statement such as "The postings on this site are my own and do not necessarily reflect the views of the organization."

UB or any work email addresses should not be used as a primary means of registering for social media sites.

In compliance with the HIPAA Privacy law, Protected Health Information (PHI) should never be posted. Something as simple as stating that you were a patient's provider is a HIPAA violation because it acknowledges that an individual was or is hospitalized or under a doctor's care. Additionally, UBMD employees should never post photos of or in relation to a patient or their care.

Clinical providers should not provide consultation or medical advice online. All UBMD employees are strongly discouraged from "friending" patients on personal social media accounts.

UBMD employees are encouraged to report violations of this policy to the UBMD Compliance Office. UBMD prohibits retaliation against any employee for reporting such violations, or for cooperating in investigations of such violations.

Should you have any questions regarding social media, contact the UBMD Compliance Office.

L. Harassment

UBMD is committed to providing a work environment in which all individuals are treated respectfully and free from harassment of any kind. This includes harassment based on race, color, gender, national origin, religion, age, sexual orientation, gender identity, disability, status as an armed services veteran or any other status protected by federal, state or local law.

Harassment is aggressive pressure or intimidation of another person or persons, often as an attempt to assert abusive, unwarranted power over them, or to negatively affect or interfere with their work, creating an intimidating, hostile or offensive work environment. Harassment includes, but is not limited to:

1. Unwelcome verbal, written, or physical conduct that denigrates or show hostility or aversion toward an individual or group because of race, color, gender, national origin, religion, age, sexual orientation, or disability (or that of an individual's relatives, friends or associates);
2. Unwelcome threats, derogatory comments, jokes, pranks, innuendoes, gestures, insults, slurs, negative stereotyping, and other similar conduct that relate to race, color, gender, national origin, religion, age, sexual orientation, or disability;

3. The placement or circulation of any unwelcome written or graphic materiel, hard copy or electronic, that denigrates or shows hostility or aversion toward an individual or group because of race, color gender, national origin, religion, age, sexual orientation, or disability.

Quid pro quo harassment is abuse of one's power, authority or position such that submission to or tolerance of such conduct is made either an explicit or implicit term or condition of employment.

Harassment of any kind, by anyone, of another individual or group is prohibited and is a violation of this Compliance Plan, and will not be tolerated. All reports of harassment, or retaliation against an employee for reporting harassment, will be thoroughly investigated, and may result in disciplinary action, up to and including termination.

M. Sexual Harassment

UBMD is committed to maintaining a workplace free from sexual harassment. All UBMD employees are required to complete annual sexual harassment training. Sexual harassment is a form of workplace discrimination. All employees are required to work in a manner that prevents sexual harassment in the workplace. This Policy is one component of UBMD's commitment to a discrimination-free work environment. Sexual harassment is against the law and all employees have a legal right to a workplace free from sexual harassment and employees are urged to report sexual harassment by filing a complaint internally with UBMD. Employees can also file a complaint with a government agency or in court under federal, state or local antidiscrimination laws.

1. UBMD's policy applies to all employees, applicants for employment, interns, whether paid or unpaid, contractors and persons conducting business, regardless of immigration status, with UBMD. In the remainder of this document, the term "employees" refers to this collective group.

2. Sexual harassment will not be tolerated. Any employee or individual covered by this policy who engages in sexual harassment or retaliation will be subject to remedial and/or disciplinary action (e.g., counseling, suspension, termination).

3. Retaliation Prohibition: No person covered by this Policy shall be subject to adverse action because the employee reports an incident of sexual harassment, provides information, or otherwise assists in any investigation of a sexual harassment complaint. UBMD will not tolerate such retaliation against anyone who, in good faith, reports or provides information about suspected sexual harassment. Any employee of UBMD who retaliates against anyone involved in a sexual harassment investigation will be subjected to disciplinary action, up to and including termination. All employees, paid or unpaid interns, or non-employees working in the workplace who believe they have been subject to such retaliation should inform a supervisor, manager, or the UBMD Chief Compliance Officer. All employees, paid or unpaid interns or non-employees who believe they have been a target of such retaliation may also seek relief in other available forums, as explained below in the section on Legal Protections.

4. Sexual harassment is offensive, is a violation of our policies, is unlawful, and may subject UBMD to liability for harm to targets of sexual harassment. Harassers may also be individually subject to liability. Employees of every level who engage in sexual harassment, including managers and supervisors who engage in sexual harassment or who allow such behavior to continue, will be penalized for such misconduct.

5. UBMD will conduct a prompt and thorough investigation that ensures due process for all parties, whenever management receives a complaint about sexual harassment, or otherwise knows of possible sexual harassment occurring. UBMD will keep the investigation confidential to the extent possible. Effective corrective action will be taken whenever sexual harassment is found to have occurred. All employees, including managers and supervisors, are required to cooperate with any internal investigation of sexual harassment.

6. All employees are encouraged to report any harassment or behaviors that violate this policy. UBMD will provide all employees a complaint form for employees to report harassment and file complaints.

7. Managers and supervisors are **required** to report any complaint that they receive, or any harassment that they observe or become aware of, to the UBMD Chief Compliance Officer.

8. This policy applies to all employees, paid or unpaid interns, and non-employees and all must follow and uphold this policy. This policy must be provided to all employees and should be posted prominently in all work locations to the extent practicable (for example, in a main office, not an offsite work location) and be provided to employees upon hiring.

What Is "Sexual Harassment"?

Sexual harassment is a form of sex discrimination and is unlawful under federal, state, and (where applicable) local law. Sexual harassment includes harassment on the basis of sex, sexual orientation, self-identified or perceived sex, gender expression, gender identity and the status of being transgender.

Sexual harassment includes unwelcome conduct which is either of a sexual nature, or which is directed at an individual because of that individual's sex when:

- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment, even if the reporting individual is not the intended target of the sexual harassment;
- Such conduct is made either explicitly or implicitly a term or condition of employment; or
- Submission to or rejection of such conduct is used as the basis for employment decisions affecting an individual's employment.

A sexually harassing hostile work environment includes, but is not limited to, words, signs, jokes, pranks, intimidation or physical violence which are of a sexual nature, or which are directed at an individual because of that individual's sex. Sexual harassment also consists of any unwanted verbal or physical advances, sexually explicit derogatory statements or sexually discriminatory remarks made by someone which are offensive or objectionable to the recipient, which cause the recipient discomfort or humiliation, which interfere with the recipient's job performance.

Sexual harassment also occurs when a person in authority tries to trade job benefits for sexual favors. This can include hiring, promotion, continued employment or any other terms, conditions or privileges of employment. This is also called "quid pro quo" harassment.

Any employee who feels harassed should report so that any violation of this policy can be corrected promptly. Any harassing conduct, even a single incident, can be addressed under this policy.

Examples of sexual harassment

The following describes some of the types of acts that may be unlawful sexual harassment and that are strictly prohibited:

- Physical acts of a sexual nature, such as:
  - Touching, pinching, patting, kissing, hugging, grabbing, brushing against another employee's body or poking another employee's body;
  - Rape, sexual battery, molestation or attempts to commit these assaults.

- Unwanted sexual advances or propositions, such as:
  - Requests for sexual favors accompanied by implied or overt threats concerning the target's job performance evaluation, a promotion or other job benefits or detriments;
  - Subtle or obvious pressure for unwelcome sexual activities.

- Sexually oriented gestures, noises, remarks or jokes, or comments about a person's sexuality or sexual experience, which create a hostile work environment.

- Sex stereotyping occurs when conduct or personality traits are considered inappropriate simply because they may not conform to other people's ideas or perceptions about how individuals of a particular sex should act or look.

- Sexual or discriminatory displays or publications anywhere in the workplace, such as:
  - Displaying pictures, posters, calendars, graffiti, objects, promotional material, reading materials or other materials that are sexually demeaning or pornographic. This includes such sexual displays on workplace computers or cell phones and sharing such displays while in the workplace.

- Hostile actions taken against an individual because of that individual's sex, sexual orientation, gender identity and the status of being transgender, such as:
  - Interfering with, destroying or damaging a person's workstation, tools or equipment, or otherwise interfering with the individual's ability to perform the job;
  - Sabotaging an individual's work;
  - Bullying, yelling, name-calling.

Who can be a target of sexual harassment?

Sexual harassment can occur between any individuals, regardless of their sex or gender. New York Law protects employees, paid or unpaid interns, and non-employees, including independent contractors, and those employed by companies contracting to provide services in the workplace. Harassers can be a superior, a subordinate, a coworker or anyone in the workplace including an independent contractor, contract worker, vendor, client, customer or visitor.

Where can sexual harassment occur?

Unlawful sexual harassment is not limited to the physical workplace itself. It can occur while employees are traveling for business or at employer sponsored events or parties. Calls, texts, emails, and social media usage by employees can constitute unlawful workplace harassment, even if they occur away from the workplace premises, on personal devices or during non-work hours.

Retaliation

Unlawful retaliation can be any action that could discourage a worker from coming forward to make or support a sexual harassment claim. Adverse action need not be job-related or occur in the workplace to constitute unlawful retaliation (e.g., threats of physical violence outside of work hours).

Such retaliation is unlawful under federal, state, and (where applicable) local law. The New York State Human Rights Law protects any individual who has engaged in "protected activity." Protected activity occurs when a person has:

- made a complaint of sexual harassment, either internally or with any anti-discrimination agency;
- testified or assisted in a proceeding involving sexual harassment under the Human Rights Law or other anti-discrimination law;
- opposed sexual harassment by making a verbal or informal complaint to management, or by simply informing a supervisor or manager of harassment;
- reported that another employee has been sexually harassed; or
- encouraged a fellow employee to report harassment.

Even if the alleged harassment does not turn out to rise to the level of a violation of law, the individual is protected from retaliation if the person had a good faith belief that the practices were unlawful. However, the retaliation provision is not intended to protect persons making intentionally false charges of harassment.

Reporting Sexual Harassment

Preventing sexual harassment is everyone's responsibility. UBMD cannot prevent or remedy sexual harassment unless it knows about it. Any employee, paid or unpaid intern or non-employee who has been subjected to behavior that may constitute sexual harassment is encouraged to report such behavior to a supervisor, manager or the UBMD Chief Compliance Officer. Anyone who witnesses or becomes aware of potential instances of sexual harassment should report such behavior to a supervisor, manager or the UBMD Chief Compliance Officer.

Reports of sexual harassment may be made verbally or in writing. A form for submission of a written complaint is attached to this Policy, and all employees are encouraged to use this complaint form. Employees who are reporting sexual harassment on behalf of other employees should use the complaint form and note that it is on another employee's behalf.

Employees, paid or unpaid interns or non-employees who believe they have been a target of sexual harassment may also seek assistance in other available forums, as explained below in the section on Legal Protections.

Supervisory Responsibilities

All supervisors and managers who receive a complaint or information about suspected sexual harassment, observe what may be sexually harassing behavior or for any reason suspect that sexual harassment is occurring, **are required** to report such suspected sexual harassment to the UBMD Chief Compliance Officer.

In addition to being subject to discipline if they engaged in sexually harassing conduct themselves, supervisors and managers will be subject to discipline for failing to report suspected sexual harassment or otherwise knowingly allowing sexual harassment to continue.

Supervisors and managers will also be subject to discipline for engaging in any retaliation.

Complaint and Investigation of Sexual Harassment

All complaints or information about sexual harassment will be investigated, whether that information was reported in verbal or written form. Investigations will be conducted in a timely manner, and will be confidential to the extent possible.

An investigation of any complaint, information or knowledge of suspected sexual harassment will be prompt and thorough, commenced immediately and completed as soon as possible. The investigation will be kept confidential to the extent possible. All persons involved, including complainants, witnesses and alleged harassers will be accorded due process, as outlined below, to protect their rights to a fair and impartial investigation.

Any employee may be required to cooperate as needed in an investigation of suspected sexual harassment. UBMD will not tolerate retaliation against

employees who file complaints, support another's complaint or participate in an investigation regarding a violation of this policy.

While the process may vary from case to case, investigations should be done in accordance with the following steps:

- Upon receipt of complaint, the UBMD Chief Compliance Officer will conduct an immediate review of the allegations, and take any interim actions (e.g., instructing the respondent to refrain from communications with the complainant), as appropriate. If complaint is verbal, encourage the individual to complete the "Complaint Form" in writing. If he or she refuses, prepare a Complaint Form based on the verbal reporting.
- If documents, emails or phone records are relevant to the investigation, take steps to obtain and preserve them.
- Request and review all relevant documents, including all electronic communications.

- Interview all parties involved, including any relevant witnesses;
- Create a written documentation of the investigation (such as a letter, memo or email), which contains the following:
  - A list of all documents reviewed, along with a detailed summary of relevant documents;
  - A list of names of those interviewed, along with a detailed summary of their statements;
  - A timeline of events;
  - A summary of prior relevant incidents, reported or unreported; and
  - The basis for the decision and final resolution of the complaint, together with any corrective action(s).
- Keep the written documentation and associated documents in a secure and confidential location.
- Promptly notify the individual who reported and the individual(s) about whom the complaint was made of the final determination and implement any corrective actions identified in the written document.
- Inform the individual who reported of the right to file a complaint or charge externally as outlined in the next section.

Legal Protections and External Remedies

Sexual harassment is not only prohibited by UBMD but is also prohibited by state, federal, and, where applicable, local law.

Aside from the internal process at UBMD, employees may also choose to pursue legal remedies with the following governmental entities. While a private attorney is not required to file a complaint with a governmental agency, you may seek the legal advice of an attorney.

In addition to those outlined below, employees in certain industries may have additional legal protections.

State Human Rights Law (HRL)

The Human Rights Law (HRL), codified as N.Y. Executive Law, art. 15, § 290 et seq., applies to all employers in New York State with regard to sexual harassment, and protects employees, paid or unpaid interns and non-employees, regardless of immigration status. A complaint alleging violation of the Human Rights Law may be filed either with the Division of Human Rights (DHR) or in New York State Supreme Court.

Complaints with DHR may be filed any time **within one year** of the harassment. If an individual did not file at DHR, they can sue directly in state court under the HRL, **within three years** of the alleged sexual harassment. An individual may not file with DHR if they have already filed a HRL complaint in state court.

Complaining internally to UBMD does not extend your time to file with DHR or in court. The one year or three years is counted from date of the most recent incident of harassment.

You do not need an attorney to file a complaint with DHR, and there is no cost to file with DHR.

DHR will investigate your complaint and determine whether there is probable cause to believe that sexual harassment has occurred. Probable cause cases are forwarded to a public hearing before an administrative law judge. If sexual harassment is found after a hearing, DHR has the power to award relief, which varies but may include requiring your employer to take action to stop the harassment, or redress the damage caused, including paying of monetary damages, attorney's fees and civil fines.

DHR's main office contact information is: NYS Division of Human Rights, One Fordham Plaza, Fourth Floor, Bronx, New York 10458. You may call (718) 741-8400 or visit: www.dhr.ny.gov.

Contact DHR at (888) 392-3644 or visit dhr.ny.gov/complaint for more information about filing a complaint. The website has a complaint form that can be downloaded, filled out, notarized and mailed to DHR. The website also contains contact information for DHR's regional offices across New York State.

Civil Rights Act of 1964

The United States Equal Employment Opportunity Commission (EEOC) enforces federal anti-discrimination laws, including Title VII of the 1964 federal Civil Rights Act (codified as 42 U.S.C. § 2000e et seq.). An individual can file a complaint with the EEOC anytime within 300 days from the harassment. There is no cost to file a complaint with the EEOC. The EEOC will investigate the complaint, and determine whether there is reasonable cause to believe that discrimination has occurred, at which point the EEOC will issue a Right to Sue letter permitting the individual to file a complaint in federal court.

The EEOC does not hold hearings or award relief, but may take other action including pursuing cases in federal court on behalf of complaining parties. Federal courts may award remedies if discrimination is found to have occurred.

In general, private employers must have at least 15 employees to come within the jurisdiction of the EEOC.

An employee alleging discrimination at work can file a "Charge of Discrimination." The EEOC has district, area, and field offices where complaints can be filed. Contact the EEOC by calling 1-800-669-4000 (TTY: 1-800-669-6820), visiting their website at www.eeoc.gov or via email at info@eeoc.gov.

If an individual filed an administrative complaint with DHR, DHR will file the complaint with the EEOC to preserve the right to proceed in federal court.

Local Protections

Many localities enforce laws protecting individuals from sexual harassment and discrimination. An individual should contact the county, city or town in which they live to find out if such a law exists. For example, employees who work in New York City may file complaints of sexual harassment with the New York City Commission on Human Rights. Contact their main office at Law Enforcement Bureau of the NYC Commission on Human Rights, 40 Rector Street, 10th Floor, New York, New York; call 311 or (212) 306-7450; or visit nwww.nyc.gov/html/cchr/html/home/home.shtml.

Contact the Local Police Department

If the harassment involves unwanted physical touching, coerced physical confinement or coerced sex acts, the conduct may constitute a crime. Contact the local police department.

N. Non-Retaliation/Whistleblowers

The UBMD Compliance Office and UBMD management shall maintain an open-door policy for employees to report problems and concerns, and assure employees that UBMD encourages the reporting of problems without fear of retaliation.

UBMD employees who report actual or potential violations or compliance concerns in good faith, regardless of whether or not a violation is found to have occurred, shall not be subject to retaliation, retribution, or harassment. No UBMD directors, officers, employees, or volunteers who in good faith report any action or suspected action that is illegal, fraudulent, or in violation of any adopted policies shall suffer intimidation, harassment, discrimination, or other retaliation or adverse employment consequences.

No UBMD directors, officers, employees, or volunteers shall engage in, or condone acts of, retaliation, retribution, discrimination or harassment against other employees for reporting compliance-related concerns. Retaliation is a violation of this Compliance Plan, and will not be tolerated. Any reports of such retaliation, retribution, or harassment will be thoroughly investigated, and may result in disciplinary action, up to and including termination.

Employees cannot exempt themselves from the consequences of wrongdoing by self-reporting. However, self-reporting may be taken into account in determining the appropriate disciplinary action.

O. Internal Investigations

The UBMD Compliance Officer or his/her designee may initiate an internal investigation for any reason, including, without limitation, testing compliance with UBMD policies and procedures, or applicable laws or regulations. Internal investigations may also be generated by irregularities identified through routine chart audits, a threat of civil litigation, a potential governmental investigation, or receipt of a subpoena. Additionally, the UBMD Compliance Officer may, at the expense of the affected Practice Plan, commence an internal investigation of any provider who has a compliance score of less than 50% on three consecutive chart audits.

Internal investigations are conducted to discover facts and circumstances surrounding alleged incidents of noncompliance, assess the legal significance of the facts discovered, evaluate the practice plan's legal rights and obligations in light of the factual conclusions reached, determine if there has been any wrongdoing, and stop any wrongdoing immediately.

Based on the findings of an internal investigation, the UBMD Compliance Officer will determine what action will be taken to correct any existing problem or potential problem. Any such action will be in accordance with Part V, Section P of this Compliance Plan.

At the conclusion of the investigation, the UBMD Compliance Officer or his or her designee will submit a report to the President of the affected Practice Plan, containing the following (if applicable):

1. Name of individual(s) being investigated;
2. Circumstances that led to the investigation;
3. Facts disclosed by the investigation;
4. List of individuals who were interviewed;
5. List of documents and records that were reviewed;
6. Internal policies, procedures, or practices that led to the violation or that could be improved;
7. The recommended course of action and options.

P. Corrective Action

As a means of facilitating the overall Compliance Plan goal of full compliance, corrective action will be recommended by the UBMD Compliance Officer if it is determined that a UBMD employee exhibits noncompliant behavior. Corrective action plans will foremost be put in place to assist the noncompliant individual in understanding the issue at hand and reduce the likelihood of noncompliance in the future. However, corrective action will effectively address the issue of noncompliance, and will reflect the severity of the noncompliant action. A plan of correction may include, without limitation:

1. Requiring mandatory educational sessions for the noncompliant individual;
2. Increasing the number and frequency of chart audits;

3. Making a repayment or voluntary disclosure to appropriate third party payers;
4. Reporting violations to the appropriate authorities;
5. Retaining an auditor, at the Practice Plan's expense, to conduct a prospective audit of each bill submitted under the provider's name until the problem has been resolved to the satisfaction of the UBMD Compliance Officer and/or the UBMD Executive Committee; or
6. Termination of employment.

Any expenses incurred as a result of the corrective action will be charged to the Practice Plan for whom the noncompliant individual works.

The UBMD Compliance Officer will recommend specific types of corrective action but no such corrective action will take effect without the written approval of the Practice Plan President. If the proposed corrective action is to be imposed on the Practice Plan President, then the approval of the UBMD Executive Committee will be required in lieu of the Practice Plan President's approval.

Q. Appeals

An aggrieved UBMD employee shall have the opportunity to appeal final recommendations made by the UBMD Compliance Officer which result in Practice Plan President determinations that noncompliance has occurred and requires corrective action. Any such appeal is exclusive of any other collective bargaining or statutory rights that may exist.

a. *Notice and Appeal* – Upon receipt of a notice of an appealable decision, the aggrieved employee shall have fifteen (15) business days to appeal the decision to the UBMD Executive Committee in writing, directed to the Chair of the UBMD Executive Committee. Written appeals not received by the UBMD Executive Committee within fifteen (15) business days shall be deemed untimely and will not be considered. The notice of appeal must contain a description of the relevant facts and a detailed explanation of the reason for the appeal.

   Upon timely receipt, the appeal shall be considered at the next regularly scheduled UBMD Executive Committee meeting provided; however, a meeting of the UBMD Executive Committee may be called sooner if the facts warrant, or at the discretion of the President. In any event, a meeting of the UBMD Executive Committee shall be held within forty-five (45) business days of the UBMD Executive Committee's receipt of an appeal. Notice of the meeting date shall be timely provided to the appellant.

b. *Submission of Documentation and Appearance* – At least three (3) business days prior to the meeting at which the appeal is to be considered, the appellant shall submit any and all documentation or materials supporting his/her appeal. The aggrieved Practice Plan member and/or provider may also request the opportunity to appear and/or be accompanied by an advocate or consultant at the meeting to present his/her position on the matter. All requests to appear shall be granted.

c. *UBMD Executive Committee* – A majority of the UBMD Executive Committee members, excluding any members in the same Practice Plan of the appellant, shall constitute a quorum for the purpose of considering the appeal. No UBMD Executive Committee member who is a member of the appellant's Practice Plan shall participate in the appeal as a member of the UBMD Executive Committee.

d. *Conduct of the Meeting* – The UBMD Executive Committee shall consider all evidence when deciding an appeal. It may also request the presence of the appellant or witnesses at the meeting to answer questions and provide additional information. The UBMD Executive Committee may review the medical record, review reports, review investigation reports, interview witnesses, and take into consideration any other material deemed necessary to make a decision. The UBMD Compliance Officer shall attend the entire meeting.

e. *The Record/Confidentiality* – The record of the appeal, which is comprised of the meeting minutes and all of the evidence, shall be considered confidential information. However, the UBMD Executive Committee may, as appropriate, disclose it to the Vice President for Health Sciences, the Dean of the School of Medicine, and the President of the Practice Plan of which the appellant is a member. The record may also be disclosed to others upon the approval of legal counsel.

f. *Written Decision* – Within thirty (30) business days of the conclusion of the hearing, a written decision shall be rendered by the UBMD Executive Committee and shall be promptly communicated to the appellant, along with the President of the appellant's Practice Plan.

g. *Further Action* – The decision of the UBMD Executive Committee is final. Following the decision of the UBMD Executive Committee, the aggrieved person shall have no further right of appeal.

R. Governmental Investigations

The Health Insurance Portability and Accountability Act (HIPAA) extended the reach of federal law to all "health care benefit programs" and provided the federal government with an array of health care crimes to investigate including:

- Health care fraud (18 U.S.C. § 1347):
- Theft or embezzlement in connection with health care (18 U.S.C. § 669);
- False statements relating to health care matters (18 U.S.C. § 1035); and
- Obstruction of criminal investigations of health care offenses (18 U.S.C. § 1518)

As such, UBMD is subject to announced and unannounced audits, surveys, and investigations by government agencies. Appropriate response to such authorized inquiries requires strict adherence to applicable laws and regulations.

Federal investigators may investigate fraud and abuse violations involving Medicare, Medicaid and other government-sponsored health plans such as worker's compensation, as well as all insurance reimbursements.

Investigators continue to concentrate on the traditional areas of fraud and abuse which have been successfully prosecuted in the past, including:

- Billing for services not rendered;
- Billing for services not medically necessary;
- Double billing for services provided;
- Upcoding (billing for a more highly reimbursed service or product than that which was provided); and
- Unlawful kickbacks and referrals.

All UBMD employees shall cooperate fully with appropriately authorized government investigations. When a government official arrives in the course of an investigation, the following steps must be followed:

- It is recommended that you notify the UBMD Compliance Officer and Practice Plan President (or administrator on call) immediately, and ask the investigator for his or her warrant before providing any documents or information;
- Request the purpose of the investigator's visit and specifically with whom the investigator desires to speak;
- Assure full cooperation with investigators within the scope of the investigation;
- Remove all non-essential personnel from the area involved in the investigation;
- Suspend any routine destruction of records during the investigation;
- Maintain a log of all events associated with the investigation;
- Staff members have the right to speak to any investigator they so choose, and have the equal right to decline to be interviewed or to ask the investigator to schedule the interview at a later date.

VI. SUMMARY OF PERTINENT LAWS, RULES & REGULATIONS

UBMD employees shall work in compliance with all applicable laws, rules and regulations. Failure to do so may result in civil and/or criminal violations, leading to exclusion, monetary fines and/or imprisonment.

A. HIPAA

HIPAA is a federal law, with civil and criminal penalties of up to $1,500,000. UBMD has a separate, detailed set of privacy, security and breach notification rules, policies and procedures, and all employees are directed to reference those policies and procedures for more comprehensive guidance on HIPAA.

The HIPAA Privacy Rule ensures the privacy of patient health care information, restricts the use and release of medical records, and gives patients more control over how that information is used. Providers are required to make a reasonable effort to protect patient privacy at all times. A patient's authorization is

required before using or releasing Protected Health Information (PHI) for purposes other than treatment, payment, or health care operations.

The Privacy Rule holds health care providers accountable for privacy violations with serious penalties for non-compliance.

The HIPAA Security Rule ensures protection of electronic Patient Health Information (ePHI). The Security Rule provides administrative, physical and technical safeguards to be followed to protect confidentiality, integrity and availability of ePHI containing patient information such as name, address, social security number, billing information and physician notes.

Administrative safeguards include setting standards on who has authorization to access ePHI; employing systems to detect, correct and prevent breaches in security; setting policies and plans for handling violations and responding to emergencies or natural disasters; creating retrievable back-up systems off site; performing ongoing evaluations and audits to ensure compliance with the Security Rule.

Physical safeguards include the implementation of access controls which limit access of ePHI, such as regularly changing passwords, PIN numbers, unique user IDs, automatic log-off, and recognized restricted areas for computers and equipment.

Technical safeguards include software technology which is often put in place by IT experts, such as virus-checking software, encryption, digital signatures and internal monitoring and audit systems.

The Breach Notification Rule requires certain notifications to be made when PHI has been improperly disclosed. UBMD follows all breach notification requirements.

B. Stark Law

The Stark Law prohibits any physician from referring patients for the provision of "designated health services" to any entity with which the physician or an immediate family member has a financial relationship, unless a statutory exception applies.

"Designated health services" are any of the following:

1. Laboratory services
2. Physical therapy
3. Occupational therapy
4. Radiology
5. Radiation therapy
6. DME & supplies
7. Nutrients, equipment & supplies
8. Prosthetics, orthotics
9. Home health services
10. Outpatient prescriptions
11. Inpatient/outpatient hospital services

If a financial relationship exists, referrals are prohibited unless a specific exception is met for both the federal and state statutes. The federal and state exceptions differ in some cases; therefore, physicians are advised against relying on the exceptions without first consulting with the UBMD Compliance Officer and/or legal counsel.

C. Antikickback Statute

The Federal Antikickback Statute creates liability for offering, providing, accepting or soliciting anything of value in exchange for the referral of business that is paid for by the Medicare or Medicaid programs.

Examples of kickbacks include waiving deductibles and copayments for Medicare patients, paying a nurse practitioner or physician a fee for referring a patient, and accepting a fee for referring a patient.

The Antikickback Statute is a criminal statute and, therefore, includes jail time as one of its penalties. Providers and their employees are prohibited from accepting kickbacks in the course of business. Additionally, providers and their employees are required to contact legal counsel or the UBMD Compliance Officer before accepting a gift or any item of value relating to or arising from UBMD business, provider relationships or medical office operations.

D. False Claims Act

The False Claims Act is a Federal statute which prohibits health care providers from "knowingly" presenting, or causing to be presented, a false or fraudulent claim for payment or approval to any federally funded program, such as Medicare and Medicaid.

The term "knowingly" does not simply refer to a specific intent to defraud the federal government. To "knowingly" present a false claim means that the provider:

1. Has actual knowledge that the information on a claim is false;
2. Acts in deliberate ignorance of the truth or falsity of the information in a claim;
3. Acts in reckless disregard of the truth or falsity of the information in a claim.

Violations of the False Claims Act may result in monetary penalties equal to three times the government's damages plus civil penalties of $5,500-$11,000 per false claim. Criminal cases may include imprisonment. Health care providers may also be excluded from participation in federal health care programs.

E. Deficit Reduction Act of 2005

The Deficit Reduction Act of 2005 States that any employer who receives more than $5 million per year in Medicaid payments is required to provide information to its employees about the federal False Claims Act, any applicable state False Claims Act, the rights of employees to be protected as

whistleblowers, and the employer's policies and procedures for detecting and preventing fraud, waste and abuse.

VII. REVISIONS TO THE COMPLIANCE PLAN

The UBMD Compliance Plan will be maintained and updated on a regular basis. It may occasionally be necessary to amend the overall structure and/or content of this Plan. In order to ensure this Plan remains viable in an ever-changing regulatory environment, and that it remains geared toward maintaining certain high standards of practice, the following procedures shall be followed with respect to changes, modifications, revisions, or amendments herein.

A. Material Changes

The UBA Executive Committee shall have exclusive authority for approving any changes to the Plan which would substantively affect the integrity of the Plan or would constitute a material change to the overall Plan. The Executive Committee on its own authority, or upon the recommendation of the Compliance Committee or Compliance Officer, shall be authorized to make material amendments, changes, modifications, or revisions to this Plan. Such revisions shall be approved upon a majority vote of the Executive Committee.

A material change is one which would result in a change to the Plan in its entirety, or which pertains to the power or authority of the Executive Committee, Compliance Officer, Compliance Committee, or revisions to any the elements of the Plan that are described in Part III. If it is unclear whether a proposed revision is material, the Executive Committee shall make the final determination.

B. Technical Changes

The Compliance Officer, upon notice to the Executive Committee, has the authority to make technical changes to the Plan which would not reduce, enlarge, or materially modify the authority of the Compliance Committee, the Compliance Officer, or the Executive Committee.

A technical change is one that is procedural in nature and has the effect of improving overall operational aspects of the Plan. Examples of technical changes include updating names or contact information and updating the Plan to reflect changes in applicable laws, rules, or regulations. A technical amendment to the Plan shall become effective upon receipt by the Executive Committee of notice from the Compliance Officer describing such changes.

ATTACHMENT A

POLICY ON CONFLICTS OF INTEREST AND DISCLOSURE OF CERTAIN INTERESTS

The position of the Officers and Directors of [INSERT NAME OF PRACTICE PLAN CORPORATION] ("PP" or the "Corporation") carry with them a requirement of loyalty and fidelity.

It is the responsibility of such persons to administer PP's affairs honestly and economically, exercising their best care, skill, and judgment for the benefit of the Corporation.

It is also the responsibility of each Director and Officer to make full disclosure of any interest that might result in a conflict on his/her part.

It is deemed to be timely and appropriate to adopt a policy on conflicts of interest for the guidance of all persons so as to ensure adherence to the policy.

NOW, THEREFORE, BE IT RESOLVED: That the following policy on conflicts of interest be hereby adopted:

1. The Directors and Officers shall exercise the utmost good faith in all transactions touching upon their duties to PP and its property. In their dealings with and on behalf of PP, they shall be held to a strict rule of honest and fair dealing between themselves and the Corporation. They shall not use their positions, or knowledge gained therefrom, in such a way that a conflict might arise between the interest of the Corporation and that of the individual.

2. All acts of such person shall be in the best interest of PP.

3. Such persons shall not accept any gifts, favors, or hospitality that might influence their decision-making or actions affecting the Corporation.

4. Although it is recognized that a degree of duality of interest may exist from time to time, such duality shall not be permitted to influence adversely the decision-making process of the Corporation. To this end, any person subject to this policy shall promptly report the possible existence of a conflict of interest for himself/herself or any other person subject to the policy. The report shall be made to the President of the Corporation.

5. The following acts are deemed conflicts of interests:

a. Outside interests

Holding, directly or indirectly, a position or a material financial interest in any outside concern from which the individual has reason to believe the Corporation secures goods or services or that provides services competitive with the Corporation. Competing, directly or indirectly, with the Corporation in the purchase or sale of property or property rights, interests, goods or services.

b. Outside activities

Rendering directive, managerial, or consultative services to any outside concern that does business with, or competes with, the services of the Corporation or to render other services in competition with the Corporation.

c. Gifts, gratuities, and entertainment

Accepting gifts, excessive entertainment, or other favors from any outside concern that does, or is seeking to do, business with, or is a competitor of, the Corporation - under circumstances from which it might be inferred that such action was intended to influence or possibly would influence the individual in the performance of his/her duties. This does not include the acceptance of items of nominal or minor value that are clearly tokens of respect or friendship and not related to any particular transaction or activity of the Corporation.

d. Inside Information

Disclosing or using information relating to the Corporation's business for the personal profit or advantage of the individual or his/her immediate family.

Full disclosure of any situation in doubt should be made so as to permit an impartial and objective determination. It should be particularly noted that disclosure relates not only to yourself but also to your immediate family.

[INSERT NAME OF PRACTICE PLAN CORPORATION]

Annual Questionnaire

Disclosure - Conflict of Interest

Pursuant to the purposes and intent of the resolution adopted by the Board of Directors requiring disclosure of certain interests, a copy of which has been furnished to me, I hereby state that I or members of my immediate family have the following affiliations or interests and have taken part in the following transactions that, when considered in conjunction with my position with or relationship to **[INSERT NAME OF PRACTICE PLAN CORPORATION]**, might possibly constitute a conflict of interest. Check "None" where applicable.

1. Outside Interest

Identify any interests, other than investments, of yourself or your immediate family which may be of conflicting interest.

None ( )

2. Investments

List and describe, with respect to yourself or your immediate family, all investments that might be within the category of "material financial interest."

None ( )

3. Outside Activities

Identify any outside activities, of yourself or immediate family which may possibly carry duality of interest.

None ( )

4. Other

List any other activities in which you or your immediate family are engaged that might be regarded as constituting a conflict of interest.

None ( )

5. Gifts, Gratuities or Entertainment

I hereby certify that neither I nor any member of my immediate family have accepted gifts, gratuities, or entertainment that might influence my judgment or actions concerning business of the Corporation, except as listed here:

None ( )

I hereby agree to report to the President of the Corporation any further situations that may develop before completion of my next questionnaire.

Name	Position	Date

ATTACHMENT B

UB|MD
PHYSICIANS' GROUP

SCRIBE AGREEMENT

I hereby certify that I have reviewed UBMD's Use of Scribes Policy and that I have received appropriate compliance and computer training allowing me to function as a scribe.

I understand that as a scribe I am to be present while the physician performs a clinical service and that I will accurately record everything the physician says during this encounter. I am not seeing the patient in any clinical capacity and must not interject my own observations or impressions.

My documentation must identify me as the scribe and attest that that the notes were created in the presence of the physician performing the service.

I am aware that documenting in the EMR requires having password access to the EMR and that documenting under some else's log in is strictly prohibited.

Name: _____

Practice Plan: _____

Signature: _____

Date: _____

Please complete and return to _____.

UB|MD
PHYSICIANS' GROUP

888-4752
UBMD Compliance HOTLINE

Taking the stress out of compliance.

COMPLETELY ANONYMOUS

- Report suspected fraud/abuse, potential problems/ concerns
- HIPAA related concerns
- Ask questions; request guidance (will need to provide contact info to receive answers)
- Provide relevant information: Date, time, department, behavior in question, person in question
- Remain anonymous if you wish
- Non-retaliation policy will be adhered to
- This is a voice mail box that will be regularly monitored during business hours
- If an **IMMEDIATE THREAT** to person or property is involved, please **DO NOT LEAVE MESSAGE** on this line - contact your direct supervisor immediately

UBMD Compliance Office

77 Goodell St., Suite 310
Buffalo, NY 14203

Larry DiGiulio,
Chief Compliance Officer

Sue Marasi,
Compliance Administrator

Peter Rossow,
Director of Audit & Education

ATTACHMENT D

COMPLIANCE ISSUE REPORT FORM

Send to: UBMD Compliance Office
77 Goodell Street, Suite 310 | Buffalo, New York 14203
Fax: 716-849-5620 | Email: smmarasi@buffalo.edu
(Email may not be anonymous)

Non-Retaliation Statement

UBMD employees who report actual or potential violations or compliance concerns in good faith, regardless of whether or not a violation is found to have occurred, shall not be subject to any form of retaliation, retribution or harassment from any UBMD officers, directors, managers or other employees.

Today's Date: _____

Please fill out the following information to the best of your knowledge.
Attach additional page(s) if necessary.

Do you wish to remain ANONYMOUS in this report? ◯ Yes ◯ No

If you are willing to provide your identity and contact information, please complete the following:

Your name: _____ Title: _____

Phone: _____ Email: _____

Practice Plan: _____ Office Location: _____

Supervisor: _____ Best time to contact you: _____

Please identify the person(s) involved in suspected behavior:

	Name	Title
(1)		
(2)		
(3)		

Have you previously reported your suspicions? ◯ Yes ◯ No

If yes, to whom (Name & Contact Info): _____

Where did this incident or violation occur? (We understand the incident may not have occurred in once specific location. However, if this incident was observed within documentation or in a business transaction, please indicate accordingly.)

_____

_____

Provide the specific or approximate date(s) the incident occurred. (Example: 9/22/17; 3 weeks ago; approximately a month ago)

_____

About how long do you think the problem has been going on? _____

How did you become aware of the violation? _____

_____

_____

Alleged Violation:

◯ **Fraud/Abuse** ◯ **Kickback/Bribe** ◯ **Stark Violation** ◯ **False Documentation**

◯ **Inappropriate Behavior (ethical)** ◯ **Unprofessional Behavior** ◯ **HIPAA Violation**

◯ **Billing for Non-Covered Services** ◯ **Billing for Services Not Performed** ◯ **Other**

◯ **Medicare** ◯ **Medicaid** ◯ **Insurance/Private Pay** ◯ **N/A or Unknown**

Please provide all details regarding the alleged violation, including location of any witnesses if relevant, facility location, and any other information that could be valuable to our office correctly identifying, evaluating and eventually resolving the specific situation. Provide as much specific detail as possible. (Attach additional sheets & supporting documents if necessary.)

_____

_____

_____

_____

FOR OFFICE USE ONLY

Date Complaint Received: _____

Result/Action Taken: ◯ No Compliance Issue Found ◯ Issue Resolved ◯ Further Action Needed

Explain: _____

_____

_____

_____

_____

_____

Add additional sheets if necessary, and attach any necessary supporting documentation.

Date Report Closed Out: _____ By (Name & Title): _____

ATTACHMENT E

COMPLIANCE PLAN AND CODE OF CONDUCT
EMPLOYEE ACKNOWLEDGEMENT

The UBMD Compliance Plan and Code of Conduct is intended to promote the highest standards of ethical care in patient care and business. UBMD is committed to full compliance with all local, state and federal health care program requirements and laws, and will not tolerate violations of applicable laws and regulations.

I acknowledge that I have received a copy of the UBMD Compliance Plan, which includes the UBMD Code of Conduct. I understand that I am responsible for reading, understanding and abiding by all policies and procedures set forth in this Compliance Plan.

I acknowledge that I have a duty to complete all required compliance training, to adhere to all local, state and federal laws and regulations that impact UBMD operations, and to immediately report any suspected violations of the UBMD policies and procedures or governmental laws and regulations to my immediate supervisor, the Compliance Officer or by utilizing the Compliance Hotline or Non-Compliance Report form.

By signing below, I agree to all of the above, and acknowledge that any violation of the UBMD Compliance Plan/Code of Conduct is grounds for disciplinary action, up to and including termination of employment.

_____ _____

Printed Name *Practice Plan*

_____ _____

Signature *Date*

Please sign and date one copy of this notice and return it to your Human Resources representative or to your immediate supervisor. You may wish to retain a second copy for your reference.

ATTACHMENT F

To print a copy, ctrl & click: NYS Language Identification Tool

NEW YORK STATE

Language Identification Tool

This chart is to assist people who do not speak or read English to identify their languages.

English
Point to your language. An interpreter will be called. The interpreter is provided at no cost to you.

Albanian — Shqip
Tregoni me gisht gjuhën tuaj. Do të thërrasim një përkthyes. Përkthyesi do të merret falas për ju.

Arabic — عربي
أشر إلى لغتك. وسوف يتم جلب مترجم فوري لك.
سيتم تأمين المترجم الفوري مجانا.

Bengali — বাংলা
আপনার ভাষার দিকে নির্দেশ করুন। একজন দোভাষীকে ডাকা হবে।
দোভাষী আপনি নিখরচায় পাবেন।

Bosnian — Bosanski
Pokažite svoj jezik. Prevodilac će biti pozvan.
Prevodilac je obezbijeđen bez troškova za vas.

Burmese — မြန်မာ
သင့်ဘာသာစကားကို ညွှန်ပြပါ။ စကားပြန် ခေါ်ပေးပါမည်။
သင့်အတွက် စကားပြန် အခမဲ့ ပေးပါမည်။

China — 請指認您的語言，以便為您提供免費的口譯服務。 请指认您的语言，以便为您提供免费的口译服务。

Cantonese	廣東話	广东话	
Chaochow	潮州話	潮州话	
Fukienese	福建話	福建话	
Mandarin	國語	普通话	
Shanghai	上海話	上海话	
Taiwanese	台灣話	台湾话	
Toishanese	台山話	台山话	

Farsi — فارسي
به زبان مورنظر اشاره کنید. ما برای شما مترجم می آوریم.
این کار هیچ هزینه ای برای شما نخواهد داشت.

French — Français
Pointez vers votre langue et on appellera un interprète qui vous sera fourni gratuitement.

German
Zeigen Sie auf Ihre Sprache. Ein Dolmetscher wird gerufen.
Dieser Service wird Ihnen kostenlos zur Verfügung gestellt.

Greek
Δείξτε τη γλώσσα σας. Θα κληθεί ένας διερμηνέας.
Ο διερμηνέας παρέχεται χωρίς χρέωση για εσάς.

Haitian Creole — Kreyòl
Lonje dwèt ou sou lang ou pale a epi n ap rele yon entèprèt pou ou. Nou ba ou sèvis entèprèt la gratis.

Hebrew — עברית
הצבע על שפתך. אנו ניצור קשר עם מתרגם.
המתרגם ניתן ללא עלות מצדך.

Hindi — हिंदी
अपनी भाषा पर इंगित करें और एक दुभाषिया बुलाया जाएगा।
दुभाषिये का प्रबन्ध आप पर बिना किसी खर्च के किया जाता है।

Italian — Italiano
Puntare sulla propria lingua.
Un interprete sarà chiamato. Il servizio è gratuito.

Japanese
母国語を示してください。通訳者が呼ばれます。通訳者が無料で提供されます。

Karen — ပှၤကညီကျိာ်
နးနဲၣ်ဃုထ့ၣ်နကျိာ်တက့ၢ်. တၢ်ကကိးန့ၢ်ပှၤတဲကျိာ်ထံကျိတၢ်.
ပှၤတဲကျိာ်ထံကျိတၢ်အံၤတလၢာ်နၤအပ့ၤဘၣ်.

Korean — 한국어
귀하께서 사용하는 언어를 지적하시면 해당
언어 통역 서비스를 무료로 제공해 드립니다.

Nepali — नेपाली
आफ्नो भाषातर्फ औंल्याउनुहोस्। एक दोभाषेलाई बोलाइनेछ।
तपाईको बिना कुनै खर्चको, एकजना दोभाषे उपलब्ध गराइनेछ।

Pashto — پښتو
خپل ژبې ته اشاره وکړۍ یو ژباړونکی به را و بللی ش
تاشو ته ژباړونکی وړیا برابر ولی شی.

Polish — Polski
Proszę wskazać swój język i wezwiemy tłumacza.
Tłumacza zapewnimy bezpłatnie.

Portuguese — Português
Indique o seu idioma. Um intérprete será chamado.
A interpretação é fornecida sem qualquer custo para você.

Russian — Русский
Укажите язык, на котором вы говорите. Вам вызовут переводчика. Услуги переводчика предоставляются бесплатно.

Somali — Afsoomaali
Farta ku fiiq luqadaada... Waxa laguugu yeeri doonaa turjubaan. Turjubaanka wax lacagi kaaga bixi mayso.

Spanish — Español
Señale su idioma y llamaremos a un intérprete.
El servicio es gratuito.

Swahili — Kiswahili
Onyesha lugha yako. Ataitishwa mkalimani.
Utapewa mkalimani bila ya gharama yoyote kwako.

Tagalog — Tagalog
Ituro po ang inyong wika.
Isang tagasalin ang ipagkakaloob nang libre sa inyo.

Thai — ไทย
ชี้ที่ภาษาที่ท่านพูด แล้วเราจะจัดหาล่ามให้ท่าน
การใช้ล่ามไม่ต้องเสียค่าใช้จ่าย

Tibetan
[illegible]

Ukrainian — Українська
Вкажіть вашу мову. Вам викличуть перекладача.
Послуги перекладача надаються безкоштовно.

Urdu — اردو
اپنی زبان پر اشارہ کریں اور ایک ترجمان بلایا جائیگا. ترجمان
کا انتظام آپ پر بغیر کسی خرچ کے کیا جاتا ہے.

Vietnamese — Tiếng Việt
Hãy chỉ vào ngôn ngữ của quý vị. Một thông dịch viên sẽ được gọi đến, quý vị sẽ không phải trả tiền cho thông dịch viên.

Yiddish — אידיש
ווײַזט אָן אויף אײַער שפּראַך און מ'וועט רופֿן אַ דאָלמעטשער. דער
דאָלמעטשער וועט צוגעשטעלט ווערן אומזיסט, עס וועט אײַך גאָרנישט קאָסטן.

Language Identity Tool (3/16)

UB|MD PHYSICIANS' GROUP

COMPLIANCE CORNER

Compliance Risks of Using APPS as Medical Scribes Office Setting 2026

Using an APP as a scribe introduces a unique set of compliance exposures because the provider is a licensed, billable clinical staff member. This creates significant risk if the role is not tightly monitored. Below is a list of compliance risks further explained.

1. **Misalignment With Scope of Practice (Major Risk)**
APPs are licensed, independent clinical practitioners. Using them as scribes may result in improper substitution, perceived clinical involvement, or unintentional clinical input. APP scribes must document only what the physician states and may not participate in the taking of the patients' history, performing physical exam, diagnosis or treatment of the patient.

2. **Risk of Double Billing or False Representation**
APPs are billable providers. Role confusion may lead to duplicate charges, improper incident-to billing, or payer assumptions that the APP contributed clinically.

3. **Attestation & Authentication Risks**
Proper scribe attestation must clarify who performed the documentation, whether the physician performed the service, and that the APP did not participate clinically. Missing or incorrect attestations create audit risk.

4. **Risk of Undocumented Clinical Contribution**
APPs may unintentionally influence care (prompting, asking clinical questions, providing impressions). This results in unbilled APP involvement and potential billing integrity issues.

5. **Obscured Medical Decision-Making (MDM)**
APP documentation may cause confusion regarding who performed the exam, made decisions, and owns the assessment and plan. This leads to downcoding or denials.

6. **HIPAA & PHI Exposure Risks**
Because APPs also perform clinical duties, they may encounter PHI beyond the scribe role or mix documentation between patients.

7. **Workforce Classification & Labor Compliance Risk**
Auditors may question whether a licensed provider is being used appropriately and whether their role aligns with HR classification, credentialing, and labor standards.

8. Training & Competency Documentation Risk
APP scribes require scribe-specific training, documentation standards training, and competency validation. Missing records creates compliance exposure.

9. Risk of Misleading Documentation
Notes may imply APP involvement, collaboration, or higher complexity, which can lead to unsupported billing.

Overall, utilizing an APP such as a Nurse Practitioner or Physician Assistant for a Medical Scribe here at UBMD is not recommended for our practice plans due to the quality of care and medical compliance risk as outlined above.

If you have any questions, please reach out to the Compliance Office for further information.

Modifier -59: Proper Usage

Modifier 59 ("Distinct Procedural Service") remains one of the most frequently misused modifiers, presenting compliance and audit risk.

Modifier 59 is consistently reviewed by our local payers and on by our local MAC NGS for Medicare. Additionally, the over utilization of Modifier 59 is discussed within our billing and coding teams on an ongoing basis. Bringing this important information and education to you will continue to keep this in the forefront of our ongoing Coding Compliance and Education Articles.

In the breakdown below we will list:

1. Common Misuse
   Across the country, a high percentage of Modifier 59 claims have historically been billed incorrectly, resulting in a high dollar amount of improper payments. This continues to influence payer scrutiny.

2. CMS and MAC Emphasis
   Modifier 59 is the most commonly appended modifier affecting NCCI (National Correct Coding Initiatives) processing, and overuse remains a known audit trigger for payers because it is an "Edit Buster" which will affect NCCI processing inappropriately. CMS recommends using X-modifiers only when appropriate.

   NCCI PTP (Procedure to Procedure) edits also define when you should not be reporting CPT codes together in all or most situations. Using a modifier 59 to "unbundle" these codes is not appropriate.

3. Trends Driving Over utilization
   - Increased coding complexity contributes to misuse.
   - Under use of X-modifiers leads to unnecessary reliance on Modifier 59. It is important to utilize the correct XE, XP, XS and XU modifier when needed.
   - Insufficient documentation remains the primary reason for incorrect use.

4. Associated Risks
   - Prepayment reviews and delayed reimbursement are common.
   - Increased denial rates related to unbundling and documentation gaps.
   - Audit exposure from MAC, OIG, and commercial payers.

5. **Best Practices – Medicare Guidance**

According to CMS' guidelines regarding appropriate and inappropriate use of Modifer -59, you should use modifier 59 or XS for different anatomic sites during the same encounter only when procedures which are ordinarily performed or encountered on the same day are performed on:

- Different organs
- Different anatomic regions
- In limited situations on different, non-contiguous lesions in different anatomic regions of the same organ

Modifiers 59 and XS are for surgical procedures, non-surgical therapeutic procedures, or diagnostic procedures that:

- Are performed at different anatomic sites.
- Aren't ordinarily performed or encountered on the same day.
- Can't be described by 1 of the ore specific anatomic NCCI PTP-associated modifiers; in other words RT, LT, E1-E4, FA, F1-F9, TA, T1-T9, LC, LD, RC, LM, or RI. See examples 1, 2, and 3 on pages 7 & 8 of the CMS Medicare Guidance booklet (https://www.cms.gov/files/document/mln1783722-proper-use-modifiers-59-xe-xp-xs-xu.pdf).

While Modifier 59 is not currently on the OIG 2026 Workplan, it has been noted in OIG investigations for over utilizations for procedures commonly unbundled and NCCI edits being bypassed.

Please review the Medicare Guidance booklet (link noted above). If you have any questions, please reach out to your Coding Team or the Compliance Office for further information.

UB|MD
PHYSICIANS' GROUP

COMPLIANCE CORNER

The Importance of Attestations

Why is proper documentation so important? When we look at patient medical records or patient claim information, it is for a multitude of reasons. Some of which are these:

- Good documentation provides quality care and promotes safety to your patients.
- Good documentation provides protection to you as the provider. It will help you avoid liability and keep you out of fraud, waste and abuse concerns.
- Good documentation is important to make sure your documentation is paid correctly. The services you provide are medically necessary and appropriately documented to reflect the work you performed on the right people.

Attestations, further provide the clarification for the work you performed and are a formal declaration, authenticity validating the statement or context of the statement.
UBMD through Allscripts offers attestations for the following documentations scenarios:

1. PATH Documentation
2. Primary Care Preceptor
3. Procedures
4. Home Visit
5. Shared Split Visit
6. Continuity of Care Visit
7. Time Billing Attestation
8. Scribe Attestations and Agreement (found in our Corporate Compliance Plan)

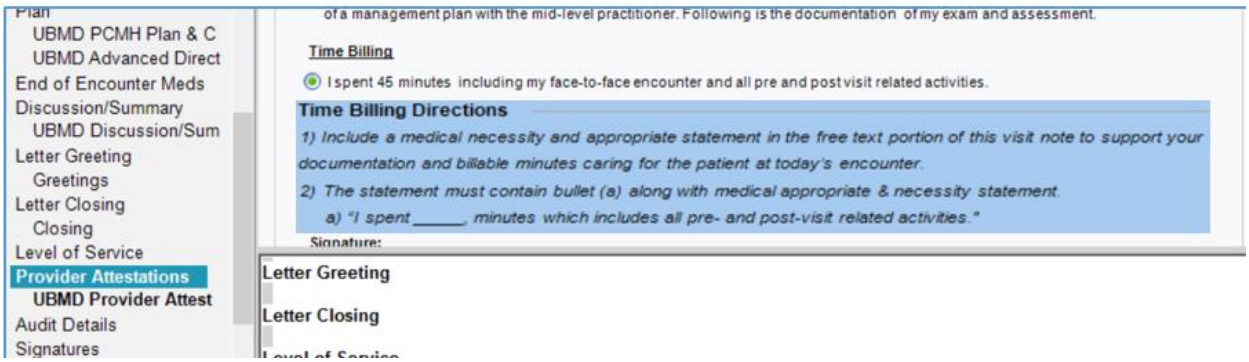
These Attestations can be found in left hand side of your Allscripts Templates drop down list under PROVIDER ATTESTIONS.

A few important reminders:

PATH Attestation is not only integral for the outpatient offices, it is necessary for the documentation in our inpatient setting. Our collaboration with local hospital affiliates also requires this as mandatory documentation for any PATH Teaching protocols when being utilized. Our hospital partners penalize us for our failure to include PATH attestations. The recommended PATH Attestation for UBMD is as follows:

"I saw and evaluated the patient. I have reviewed the patient history, exam, and care plan with the Resident/Fellow and agree with the findings and recommendations as detailed above on (date of service)".

Time Attestations:

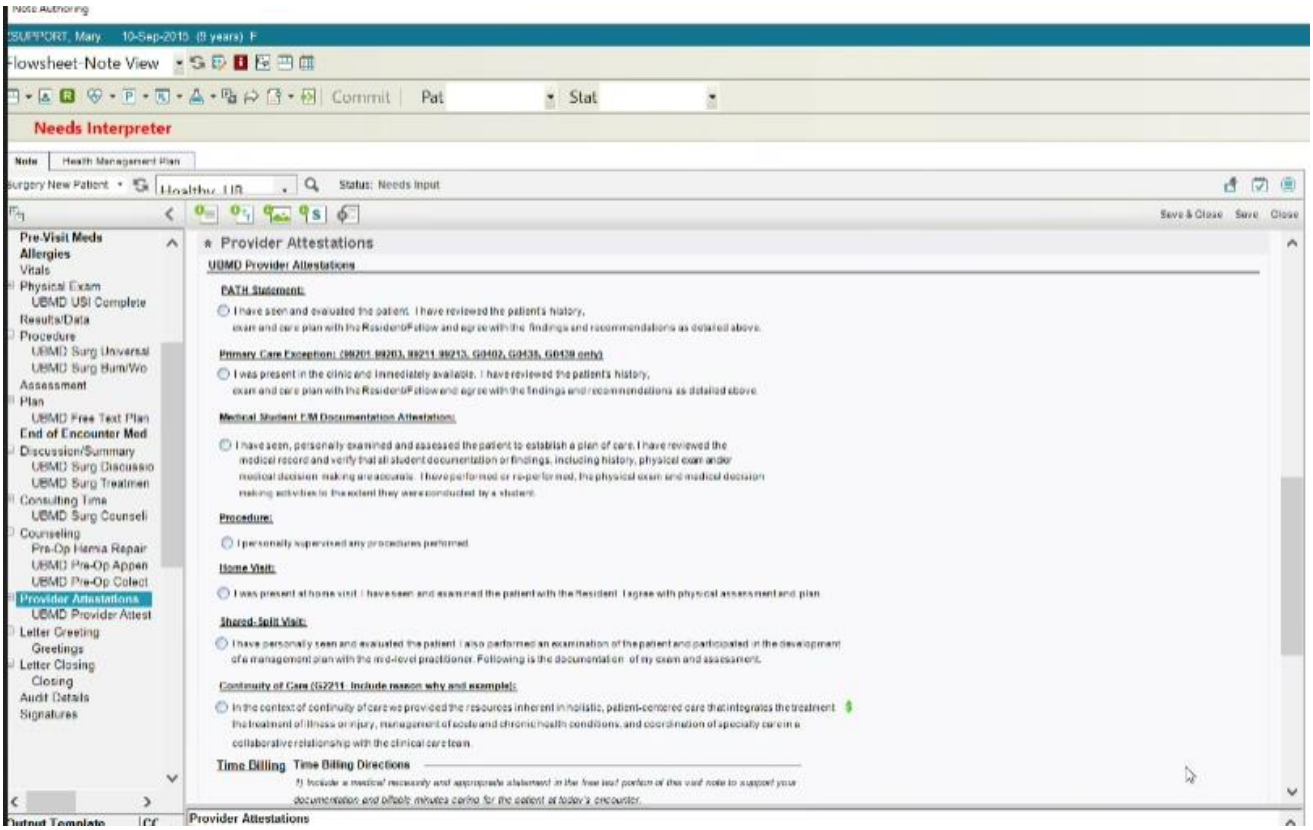


When Time is used for reporting E/M service codes, the time is defined by your documentation. It is used to select the appropriate service level. It must be distinct and noted in the patient's chart.

Once you have the total time spent on the encounter date, it should be documented in the medical record and used as the basis for code selection **IF** you are utilizing TIME as the basis for your coding. In the FREE TEXT portion document, the medical necessity and make sure you account for any "carve out" procedures from your total time.

Reference in Allscripts – Attestations:

Please see the screen shot for your reference for the noted Attestations for Allscripts practice plans.



It is imperative that ALL compliant attestations must be noted on documentation. These attestations document each scenario for different patient visits. Without these attestation proper documentation, billing and coding services cannot be compliantly billed and coded.

If you have any further questions regarding Attestations, please reach out to the Compliance Office for further information.

Anti-kickback Statute vs. Stark Law: A Practical Comparison

Sometimes navigating federal regulations in healthcare can feel like walking through a legal minefield. Two of the most challenging "mines" are the **Anti-Kickback Statute (AKS)** and the **Stark Law**. Both share the goal of preventing financial gain from influencing medical decisions, but they operate very differently.

The Anti-Kickback Statute (AKS)

The AKS is a broad **criminal law** that prohibits the exchange (or offer) of anything of value—referred to as "remuneration"—to induce or reward the referral of business reimbursable by federal healthcare programs (like Medicare or Medicaid).

- **Intent:** To be convicted, the government must prove that the parties involved *intended* to swap money or favors for referrals.
- **Scope:** It applies to anyone (doctors, hospitals, laboratories, drug reps, even patients) who can influence a referral.
- **Safe Harbors:** Because the law is so broad, the government created "Safe Harbors" for specific business arrangements that are immune from prosecution if they meet strict criteria.
    - **Space & Equipment Rental:** Must be in writing, for at least one year, and rent must be Fair Market Value (FMV) and not based on volume of referrals.
    - **Personal Services & Management Contracts:** Must be in writing, for at lease one year, with compensation set in advance at FMV.
    - **Investment Interests:** Protects returns on investments in large publicly traded companies or small entities (if strict ownership and revenue rules are met).
    - **Bona Fide Employees:** Payments made by an employer to a true W-2 employee for employment in the furnishing of any item or service.
    - **Discounts:** Protects certain price reductions if they are properly disclosed and reflected in costs claimed by the provider.
    - **Practitioner Recruitment:** Helps hospitals recruit doctors to underserved areas. Requires the doctor to relocate and the hospital not to demand referrals.

The Stark Law (Physician Self-Referral Law)

The Stark Law is a **civil statute**. It prohibits a physician from referring Medicare or Medicaid patients for **Designated Health Services (DHS)** to an entity with which the physician (or an immediate family member) has a financial relationship.

- **Intent:** It doesn't matter if you intended to break the law. If the financial relationship exists and doesn't fit into an exception, you are in violation.
- **Scope:** Only applies to physicians and their immediate family members.
- **Exceptions:** Unlike AKS safe harbors (which are voluntary), Stark Law exceptions are mandatory. If an arrangement doesn't meet an exception perfectly, the referral is illegal.
- **Designated Health Services** include:
  - Lab tests
  - Physical, occupational, and outpatient speech-language therapy
  - Radiology and imaging (MRI, CT, ultrasound)
  - Radiation therapy and supplies
  - Durable Medical Equipment (DME) and supplies
  - Nutrient, equipment, and supplies
  - Prosthetics, orthotics, and supplies
  - Home health care
  - Outpatient prescription drugs
  - Inpatient and outpatient hospital care

Side-by-Side Comparison

Feature	Anti-Kickback Stature (AKS)	Stark Law
Legal Nature	Criminal & Civil	Civil
Standard of Proof	Knowing and Willful (Intent matters)	Strict Liability (Intent is irrelevant)
Applicability	Anyone who refers/induces referrals	Physicians and immediate family members
Scope	All Federal Healthcare Programs	Medicare and Medicaid
Prohibited Acts	Kickbacks for any item or service	Self-referrals for "Designated Health Services"
Penalties	Prison, fines, and program exclusion	Fines, repayments, and program exclusion

While AKS and Stark Law have different legal mechanics, both aim to ensure that medical decisions are driven by what the patient needs, not by who is getting paid. Some common goals both have include:

- Protecting Clinical Judgment
  If a doctor receives a financial bonus for referring a patient to a specific lab or imaging center, there is a risk that the referral is being made for the money rather than the quality of care. These laws aim to keep the patient-provider relationship genuine.
- Preventing Overutilization
  When financial incentives are involved, there is a natural tendency to order more tests, procedures, or prescriptions than are strictly necessary. This can put patients through unnecessary medical stress and can drain the resources of taxpayer-funded programs.
- Controlling Healthcare Costs
  Overutilization and steered referrals directly lead to higher costs for Medicare and Medicaid. By removing the financial incentive that drives unnecessary referrals, these laws help keep federal healthcare spending from spinning out of control.
- Ensuring Fair Competition
- In a healthy market, providers compete based on quality, convenience, and price. Kickbacks and self-referrals create a "pay-to-play" environment where smaller or higher-quality providers might be pushed out because they aren't participating in the same financial schemes.
- Preserving Public Trust
  AKS and Stark are about maintaining the integrity of the healthcare system. Patients need to trust that when their doctor says, "You need this MRI," it’s because they actually need it, not because the doctor owns a piece of the MRI machine down the hall.

The Anti-Kickback Statute and the Stark Law may feel like two distinct legal hurdles, they actually work together for the same common goal. The AKS targets the "why" by focusing on criminal intent and illicit exchanges, while the Stark Law addresses the "what" through strict liability for specific physician relationships. Despite their different mechanics, their singular mission is to ensure that when a patient receives a referral, it is rooted in **medical necessity** rather than a profit margin. Staying compliant isn't just about avoiding heavy fines or prison time, it’s about safeguarding the integrity of the healthcare system and our practices, and ensuring that clinical judgment remains focused entirely on the patient.

HIPAA: Importance of Secure Passwords

Under HIPAA, healthcare providers are required to implement technical safeguards to protect ePHI. One of those safeguards is the use of passwords, which really are the frontline of defense against data breach. If that line breaks, it is not only data at risk, but your patients' trust and your practice's legal standing.

A single compromised password can lead to a massive data breach. For a healthcare worker, this can result in:

- **Patient Harm:** Unauthorized access can lead to tampered records or identity theft.
- **Legal Consequences:** HIPAA violations can carry hefty fines, sometimes reaching millions of dollars.
- **Career Impact:** Negligence in handling credentials can result in corrective action including termination, exclusion, or loss of license.

In February, HHS-OCR announced a $1,500,000 civil monetary penalty against Warby Parker, Inc. ("WPI") in a HIPAA cybersecurity hacking investigation. In 2018 they received a breach report filed by WPI regarding unauthorized access by one or more third parties to customer accounts. The report stated that WBI became aware of unusual attempted log-in activity on its website. WPI reported that between September 25, 2018 and November 20, 2018, unauthorized third parties gained access to WPI customer accounts by using usernames and passwords obtained from other unrelated websites that were presumably breached. 197,986 individuals were affected by the breach.

To stay compliant and secure, there are many guidelines for selecting passwords and for password usage. First and foremost, you should NEVER reuse passwords.

- Never use your UB name and/or password for a non-UB IT service. If that service is compromised, then your UB credentials are at risk.
- Never reuse passwords. For example, your Netflix password should never be the same as your password to log into the Electronic Medical Record (EMR) system.

When creating a password, the University at Buffalo ("UB") requires:

- A capital letter
- At least 1 number
- Special characters (i.e., period at the end of the sentence, spaces between the words, *, #)
- No more than 32 characters
- No personal information

UB also suggests using a passphrase rather than a password as they are more secure and can be easier for you to remember. A passphrase is a sentence that includes capitalization, spaces, punctuation and at least one number. The example they give is "Sunshine on my shoulder," which meets all the UB requirements mentioned above.

Cyber-attackers get your information in many ways, including but not limited to:

- **Malware (Malicious Software):** Common types include viruses, worms, ransomware, and spyware. It acts as a digital parasite, stealing data, spying on users, or locking systems for ransom.
- **Phishing:** Attacker impersonates legitimate organizations via email, text message, or phone to steal sensitive information such as passwords, PHI, credit card numbers, or other data. They use urgent, deceptive messages to lure you into clicking malicious links or opening attachments.
    - Look for urgent or threatening language, poor grammar and spelling, and/or mismatched sender email address that don't match the domain of the organization.
- **Cracking:** Cracking programs automatically guess common or simple passwords or phrases first and can make over one million attempts per second.

Final Do's and Don'ts to stay compliant and secure, and to help deter cyberattacks:

- **DO Use Multi-Factor Authentication (MFA):** Even if a hacker steals your password, MFA provides a second barrier (like a code sent to your phone) that is much harder to bypass.
- **DO Use "Passphrases":** Instead of P@ssw0rd1!, try a long string of random words like Blue-Giraffe-Coffee-2026! They are easier for you to remember but significantly harder for "brute-force" software to crack.
- **DO Change Default Passwords:** If you are issued a temporary password for a new system, change it at your first login.

****

- **DON'T Share Credentials:** Your login is your digital signature. If someone else uses your account to access a file, HIPAA logs will point to *you* as the one who viewed it.
- **DON'T Use "Sticky Note" Security:** Never write your password on a Post-it and stick it to your monitor or hide it under your keyboard. In a busy clinic, anyone walking by - including patients - could see it.
- **DON'T Reuse Passwords:** Your Netflix password should never be the same as your access code for the Electronic Health Record (EHR) system.
- **DON'T Leave Stations Logged In:** Always lock your computer when stepping away from your desk, even for a "quick second."

COMPLIANCE CORNER

Your Role in Healthcare Compliance

Compliance in healthcare is essential because it serves as the foundation for protecting patient safety, securing personal data, and ensuring financial integrity. Without strict adherence to rules, regulations, and policies, UBMD practices and/or individual personnel face severe consequences that can range from fines to imprisonment to exclusion.

Key Reasons for Healthcare Compliance:

- **Ensuring Patient Safety & Quality of Care**: Compliance programs establish standard operating procedures that mitigate medical errors, mismanagement, and unsafe clinical practices.
- **Protecting Patient Privacy**: Under regulations like HIPAA, organizations must safeguard sensitive health information from unauthorized access, misuse, or cyberattacks. This builds essential trust between patients and providers.
- **Preventing Fraud, Waste, and Abuse**: Strict billing and coding regulations, such as the False Claims Act, prevent organizations from overcharging the government or private insurers for services. This preserves critical funding for programs like Medicare and Medicaid.
- **Mitigating Legal and Financial Risks**: Non-compliance can lead to devastating penalties, including:
  - **Fines**: Fines can reach millions of dollars.
  - **Imprisonment**
  - **Exclusion from Programs**: Providers may be barred from participating in federal programs like Medicare and Medicaid, which can cripple practice revenue.
  - **License Revocation**: Individual practitioners risk losing their professional licenses, effectively ending their careers.
- **Upholding Ethical Standards**: Compliance frameworks like Anti-Kickback Statute and Stark Law prevent conflicts of interest, ensuring that medical decisions are based purely on patient needs rather than financial gain for the provider.

As UBMD executives, providers and staff, you are essential to upholding compliance within our organization. Your daily tasks put you on the front lines of compliance. Your roles include following established policies, participating in training, identifying potential violations, and reporting concerns through proper channels to maintain organizational integrity and mitigate risks.

Key Roles and Responsibilities of Executives, Providers, and Staff:

- **Adherence to Policies:** You are responsible for understanding and actively following internal policies and procedures and federal/state laws.
- **Training and Education:** You must participate in mandatory training to stay current on compliance risks, policies, rules, and regulations.
- **Reporting Concerns:** You are required to report **known or suspected** non-compliance, fraud, or unethical behavior to a supervisor and/or the UBMD Compliance Office directly or via the Compliance Office hotline. Retaliation for reporting compliance concerns in good faith will not be tolerated, regardless of whether or not a violation is found as a result of the initial report.
- **Billing Accuracy:** You must ensure that documentation supports the billing codes used, preventing fraudulent claims.
- **Protecting Patient Rights:** You must consistently uphold patient confidentiality and safety standards in daily operations.
- **Participating in Audits:** You must cooperate with internal reviews and audits conducted by compliance personnel to identify areas for improvement.

Failure to uphold these responsibilities can result in disciplinary action up to and including termination.

Compliance Hotline

716.888.4752

An open line of communication between the UBMD Compliance Office and all practice plan personnel is an imperative part of a successful compliance program. In an effort to enhance communications, we have a Compliance Hotline in place.

Practice personnel can call 716-888-4752 any time to report **known or suspected** fraud, abuse, HIPAA-related or other compliance concerns, or to ask any questions or request guidance in compliance matters.

Callers may remain anonymous if desired. It is our policy to preserve anonymity of callers who wish to remain anonymous, subject to limits imposed by law. But you may include your name and contact information if you wish to.

You are asked to provide all relevant, detailed information regarding the incident(s), such as:

- Date(s) and time(s) of incident(s)
- Department/location
- Behavior in question
- Person(s) involved

Hotline calls will go to a non-traceable voice mailbox, which will be monitored by UBMD Compliance Office personnel during regular business hours, 8:00am-5:00pm Monday through Friday. However, the hotline is accessible 24 hours, 7 days a week, allowing callers to leave a message no matter when they call. All calls to the hotline will be confidential, and no attempt will be made to determine the number or location of the caller.

NOTE: If there is an **IMMEDIATE THREAT** to person or property, you should not leave a message on the hotline. You should instead contact your direct supervisor immediately.

Ctrl + Click here for a printable flier with further hotline information. Copies of the flier should be displayed in common employee areas at all of your practice sites.

UB|MD
PHYSICIANS' GROUP

UBMD COMPLIANCE HOTLINE

716-888-4752

COMPLETELY ANONYMOUS

- Report known, suspected or potential fraud, abuse, problems, concerns.
- Report HIPAA-related concerns.
- Report other compliance issues or concerns.
- Ask questions; request guidance (you will need to provide contact info to receive answers).
- Provide relevant information: Date(s), time(s), department, behavior in question, person(s) in question.
- You are welcome to provide contact information if you wish, but you may remain anonymous if preferred.

UBMD Compliance Office

665 Main St., 2nd Floor
Buffalo, NY 14203

Larry DiGiulio,
Chief Compliance Officer

Sue Marasi,
Compliance Administrator

- UBMD's non-retaliation policy will be strictly adhered to.
- This is a voice mail box that is monitored during regular business hours, but is accessible for reporting 24 hours, 7days a week.
- If there is an **IMMEDIATE THREAT** to person or property, please **DO NOT LEAVE MESSAGE** on this line.

  Contact your direct supervisor immediately!

2026 Staff/Non-Provider Training Attestation for New & Existing Personnel

I attest that I have received and read the following training materials as part of my new employee orientation or annual training as an employee of a UBMD Physicians' Group practice.

I attest that I understand the content of these materials and agree to maintain ongoing compliance with any and all applicable policies, procedures and requirements.

I further attest that I will incorporate the principles and requirements of this training into my daily work practices. Additionally, I understand that I may be held accountable for any and all of my actions or omissions that conflict with the information and standards provided in this training program.

- ☐ Fraud, Waste & Abuse PowerPoint Training
- ☐ HIPAA PowerPoint Training
- ☐ Telemedicine Updates 2026
- ☐ Cultural Competency – Think Cultural Health
- ☐ UBMD Compliance Plan
- ☐ Compliance Corner Articles
  - Compliance Risks of Using APPs as Medical Scribes
  - Modifier -59 Proper Usage
  - The Importance of Attestations
  - Anti-kickback vs. Stark Law
  - HIPAA: The Importance of Secure Passwords
  - Your Role in Healthcare Compliance
- ☐ UBMD Compliance Hotline
  - UBMD Compliance Hotline Statement
  - UBMD Compliance Hotline Flier

◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊◊

After reviewing **all** required trainings listed above, you must complete the brief quiz following this page (you will need to keep the question page in front of you).
To do so, go to https://smbsweb.med.buffalo.edu/ubmd/training.aspx and select "2026 **Staff and Non-Provider** Compliance Training" from the Training Module dropdown menu.

- Enter your UBIT Name if you have one. If not, leave blank.
- Enter your Last Name, First Name and select the practice plan that you are employed by.
- Select your answers to **all** questions, then click "Submit Answers"

- If all answers are correct, you will see a screen stating: *"Data Submitted. Congratulations your responses have been submitted."*
- If any answers are incorrect, you will see a screen stating: *"It appears you have some incorrect responses. You should check your answers to Question #_____."*
    - You should then click "OK" and correct your answer(s).
- All answers must be correct to receive credit.

** Important Additional Training Notes **

1. **Sexual Harassment Prevention Training (SHP)**
   Because SHP training is done in collaboration with our hospital partners, it will be sent out later in the year as always. Please remember that you should **not** complete the University's SHP training when you receive it and should instead wait to receive the UBMD/Hospital SHP training which will be forwarded to you by UBMD Compliance Administrator, Sue Marasi, as soon as it is available.

2. **Title VI and Workplace Violence & Bullying Prevention Training**
   This training will be sent out later in the year by the University, and is completely separate from our UBMD Compliance training program. Any questions regarding Title VI and Workplace Violence & Bullying Prevention Training should be directed to the person who sends the email for them.

3. **Active Shooter Training**
   While this is not a mandatory part of our training, we strongly recommend that you view the video recorded by UB University Police force. You can find the video on our UBMD Compliance Office website at:

   https://www.ubmd.com/about-ubmd/Compliance/Education-training.html

2026 Compliance Training Quiz

FWA

1. Knowingly billing for services of higher complexity than services actually provided or documented is an example of:

a. Fraud
b. Waste
c. Abuse
d. All of the above

2. Prescribing more medications than necessary to treat a specific condition is an example of:

a. Fraud
b. Waste
c. Abuse
d. All of the above

3. Beyond paying restitution to CMS for fraudulently obtained payments, fraud and abuse penalties can include exclusions, civil monetary penalties, and sometimes criminal sanctions, which include fines and prison, against health care providers and suppliers who violate which of the following:

a. False Claims Act
b. Anti-Kickback Statute
c. Stark Law
d. Fraud Statute
e. All of the above

Stark

4. An important difference between the Anti-Kickback Statute and Stark Law is that intent matters to prove violation of the AKS and is irrelevant for showing violation of the Stark Law.

a. True
b. False

Scribes

5. If using an APP as a scribe, proper scribe attestation must clarify who performed the documentation, whether the physician performed the service, and that the APP did not participate clinically.

a. True
b. False

HIPAA

6. If a minor over the age of 12 objects to the disclosure of medical information to their parent, the provider has the discretion to **deny the parent's request** for access, provided the provider believes disclosure would be detrimental to the provider-patient relationship or the minor's care.

a. True
b. False

7. Modifier 59 ("Distinct Procedural Service") remains one of the most frequently misused modifiers, presenting compliance and audit risk.

a. True
b. False

8. This is the correct UBMD PATH attestation: "I saw and evaluated the patient. I have reviewed the patient history, exam, and care plan with the Resident/Fellow and agree with the findings and recommendations as detailed above on (date of service)".

a. True
b. False

9. Providers can bill for telehealth for the delivery of biopsy results, MRI results, blood work results, and test results.

a. True
b. False

Attestation

10. By selecting answer "a. Yes" below, you are signing the attached attestation regarding completion and understanding of the 2026 UBMD Compliance Training Program.

a. Yes